Thesis Title:

Digital Regulation Contested—
Regulatory Approaches of the U.S., the EU, and China to Cross-Border Personal Data Transfers

Candidate's Name:

Gao, Yang (Raymond)

Time of Submission for Examination:

February, 2023

A thesis submitted for the degree of Doctor of Philosophy (PHD)
of the Australian National University

Copyright by Gao, Yang (Raymond) 2023 (all rights reserved)

Statement

This thesis is solely completed by me and is my original work. To the extent that I made reference to existing scholarship or commentaries, I have cited the relevant sources in the footnotes. I have not engaged any third-party editorial services to edit or proofread my thesis. Any chapter of this thesis has not been published at academic journals as of the submission date. Among various chapters, Chapter 1 was presented at the 2021 American Society of International Law Research Forum in November, 2021, and Chapter 2 was presented at the 2022 Junior Faculty Forum of Journal of International Economic Law in September, 2022.

Acknowledgements

I would like to express my sincere gratitude to my thesis supervisors: prof. Anthea Roberts (ANU, RegNet), Susan Sell (ANU, RegNet), Heng Wang (Singapore Management University, School of Law), and Henry Gao (Singapore Management University, School of Law). I am grateful for their valuable guidance, mentoring, and encouragement during this research project. I am heavily indebted to their academic works, theories and insights, comments and feedbacks, and various support that helped me throughout this journey. This thesis was funded by the Australian Government Research Training Program Scholarship.

Abstract

In the unfolding digital era, the regulatory battles over international personal data transfers have increasingly come to the foreground of great power rivalry, substantially shaping the emerging transnational data governance system. Focused on transnational regulation of cross-border personal data transfers for commercial purposes, this thesis delved into the creation, development, and diffusion of three distinct regulatory approaches, which have been advanced respectively by the U.S., the EU, and China (the "Big Three").

First, this thesis unpacks three primary (yet not mutually exclusive) conceptualizations of personal data, and discusses their normative implications for the regulatory design to govern this contentious issue-area. Aligned with their respective policy preferences, the U.S., the EU, and China adopt disparate primary conceptualizations of personal data—as a factor of production, an embodiment of fundamental rights, and an element of national security, respectively. Emphasizing a particular attribute of personal data and playing down others, such conceptual framings differ in what they characterize as the most prominent interests at stake, in how they organize the underlying relationship between individuals, their data, and the governments, and in what they frame as the most important policy objectives for regulatory interventions. Embedded in different ideologies and philosophies, these conceptualizations contain irreducible normative components—ranging from neoliberalism to human rights and to state sovereignty—making the regulatory contestations over cross-border data flows highly complex. Moreover, different conceptual framings mandate and justify competing legal paradigms to regulate this issue-area, which diverge in their basic logic, normative justifications, policy priorities, as well as legal and regulatory solutions.

Second, drawing on international relations (IR) literature on the analysis of regime complexity, this thesis explores the evolution and development of the U.S., the EU, and China's regulatory approaches to govern cross-border personal data flows. It conceptualizes the emerging legal and regulatory framework governing this issue-area as a transnational regime complex. Absent universal rules or multilateral institutions devoted to regulating international data transfers, different sets of international, regional, and domestic institutions have been vying to dominate the governance of this multi-faceted and cross-cutting issue-area. In this context, the Big Three have been deploying competitive lawmaking strategies of "regime-" and "forum-shifting" to shape the emerging rules on their preferred terms. Unable to sufficiently advance their preferred interests at the existing multilateral venues, these great powers have been shifting the rulemaking processes to an international trade regime, a regional data protection regime, and domestic security-oriented institutions, respectively. By setting the terms for cross-border personal data flows, these great powers strive to shape the transnational rulemaking processes in ways that reflect their visions, serve their prioritized interests, and take advantage of their institutional capacities.

Third, in the global regulatory environment, these three primary governance approaches to cross-border data flows have been increasingly diffusing among third countries—whether through a great power's norm promotion efforts, the ideational power of the norms themselves, or otherwise. Drawing on policy diffusion theory, this thesis explores the mechanisms and factors driving third countries' increasing emulation and adoption of the U.S., European, and Chinese regulatory approaches, explaining the emergence of three regulatory "spheres of influence" worldwide.

TABLE OF CONTENTS

Introduction 5

Research Design of This Project

Chapter 1 30

A Battle of the Big Three?
Competing Conceptualizations of Personal Data
Shaping Transnational Data Flows

Chapter 2 88

U.S.-Led Regime- and Forum-Shifting—
The Rise and Rule of a Trade-Based Approach to
International Personal Data Transfers

Chapter 3 125

Forum Shifting to Regulate Data Privacy—
The Creation and Evolution of EU Data Protection Regulation

Chapter 4 195

Implications of EU Data Protection Law
for the Transnational Regime Complex
Governing Cross-Border Personal Data Transfers

Chapter 5 227

"Data Sovereignty" Unchallenged?
The Evolving Domestic Data Governance Regime of China
and Its International Implications

Chapter 6 298

Policy Diffusion of the Chinese Approach to Cyber and Data Governance

Chapter 7 334

Concluding Remarks

Bibliography 349

Introduction:

Research Design of This Project

Today, data has become a ubiquitous buzzword in policy debates, legal discussions, and our daily lives. As the pervasive tide of "digitalization" unfolds, our personal data has increasingly become almost everywhere and anywhere, traveling across national borders at lightning speed in a fashion that is often unknown, undetectable, and even inconceivable to us. Notably, data becomes increasingly crucial for digital trade, the data-driven economy, cutting-edge technologies, civil liberties and privacy, and national security, creating novel and complex regulatory challenges for policymakers, firms, individuals, and various stakeholders.

In this context, the regulatory battles among great powers over transnational data governance increasingly intensify, as they compete to establish the rules for cross-border personal data transfers. From the perspective of international economic governance, this thesis explores the emerging transnational legal and regulatory framework that governs cross-border personal data flows. Through comparative case studies of the U.S., the EU and China (the "Big Three" or three "great powers"), it surveys three major sovereign actors' distinctive pathways of transnational rulemaking. Specifically, it delves into their respective conceptualizations of personal data, the factors driving their divergent approaches, the lawmaking strategies deployed to push for their preferred rules, the diffusion of their norms in the global regulatory arena, as well as the implications for the transnational digital order.

Table of Contents

I. WHY THIS PROJECT? 6

A. Transnational Personal Data Flows..... 6

(A) Data Is the New Oil 7

(B) Data Is Different 8

B. Three Great Powers Across the Globe..... 10

C. The Global Regulatory Arena for Great Powers..... 11

E. How is the Emerging TPDF Framework Different?..... 11

II. CORE RESEARCH QUESTIONS 13

III. THEORIES AND METHODS..... 14

A. Discursive Analysis 14

B. International Relations Theories of Regime- and Forum-Shifting 16

C. Policy Diffusion Theory..... 18

D. Empirical Sources..... 20

IV. CONTRIBUTIONS TO THE EXISTING LITERATURE..... 20

V. CAVEATS OF THE RESEARCH 27

VI. A ROADMAP OF THE PROJECT 27

I. WHY THIS PROJECT?

As its center, this project is mainly concerned with three dominant regulatory approaches—each advanced by one of the U.S., the EU, and China—to govern transnational personal data flows ("TPDF"), and it approaches this topic primarily through the lens of global economic governance. This section illustrates the reasons for this project's focus.

A. Transnational Personal Data Flows

Regulatory struggles over cross-border information flows are nothing new. Hardly unprecedented in history, the current regulatory contestations over transnational personal data transfers is reminiscent of the legal and policy debates in the 1990s over whether the Internet would defy territorial regulations or become bordered under territorial-based controls and coercion of national governments.[1] At that time, many Internet advocates and activists argued that the Internet should, by virtue of its nature as a borderless medium, escape geography, defy territorial regulations, and become a self-governing regime serving the public good.[2] In contrast, others foresaw that the Internet would become a geographically bordered network, splitting apart to conform to the jurisdictional rules and governmental control of different states.[3] For better or for worse, history found in favor of the latter view, and nowadays states have been increasingly tightening their territorial-based regulatory control over the Internet.[4]

Nevertheless, this time the regulatory clash over transnational personal data transfers is in many ways more *consequential* and *contentious* than that historical antecedent. In the unfolding wave of digitalized revolution, data is hailed as the "new oil" fueling the data-driven economy and transformative technologies.[5] The legal and regulatory framework governing cross-border data flows has the potential to drastically mold the arteries of digital trade, data-driven services, and the digital economy, with paramount importance for the global tech race and geo-economic rivalry among major powers. These aspects evidence the immense distributional effects of the current regulatory battle over data governance.

Meanwhile, with its distinctive characteristics, data raises novel, important, and challenging questions that are starkly different from those brought about by other traditional factors of production. Due to its novel and hybrid nature, personal data is subject to three primary conceptualizations, ranging from economics to privacy to national security.[6] Whereas the previous Internet debate largely struggled with a *binary* choice between an "unterritorial" and a "territorial-based" version of the Internet, this time the regulatory contestations on cross-border personal data

---

[1] Jennifer Daskal, *Borders and Bits*, 71 VANDERBILT LAW REVIEW 179, 181 (2018).
[2] See *e.g.*, David R. Johnson & David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).
[3] See e.g., JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).
[4] Daskal, *supra*, 181.
[5] *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[6] See *infra* chapter 1 ("A Battle of the Big Three"), section II.

flows largely revolve around *three* competing regulatory approaches, each emphasizing a different attribute of personal data and each advanced by a great power. With three dueling visions competing for global dominance, the regulatory clash remains highly contentious.

(A) Data Is the New Oil

As noted earlier, data has been acclaimed as the "new oil" in the digital era. Capable of powering lucrative and fast-growing digital industries, the economic and strategic value of data could not be more profound.

Economically, data represents the lifeblood of the modern global digital economy, manifesting enormous potentials for boosting revenues, economic efficiency, productivity, and innovation. For the data-driven economy based on the collection, storage, processing, analysis, exchange, transfer, and exploitation of digital information ("data"), "big data" gleaned from the Internet and digitally connected devices (the "Internet-of-Things") constitutes an indispensable intangible factor of production. Notably, data fuels smart manufacturing, the sale of goods, the provision of digital services, international trade, and trade in data in itself (such as predicative analytics and targeted advertisement services).[7] Firms whose business models center on data-driven services are often heavily dependent on data, much of which is personal data (i.e., data by and about people).[8]

Strategically, big data serves as an important raw material to train and develop Artificial Intelligence ("AI") and other cutting-edge technologies that are substantially driven by data (such as machine learning, automation, predictive analytics, robots, and 3D printing).[9] Importantly, there exists a reciprocal relationship between big data and such transformative technologies. While cutting-edge technologies often depend on data to achieve greater success, they also enable data to unlock new possibilities that were previously infeasible.[10] Such reciprocal dynamics often embody a positive feedback loop: the more the data, the better the products and technology, which would snowball into greater data collected from more users and customers, which in turn would further improve the products and technology, and so on.[11]

In this context, data becomes a vital resource with prime strategic importance. In the global tech race, who controls what data and how this is utilized may determine which country can take the lead in mastering AI-powered transformative technologies, shaping global value chains, national competitive advantages, the relative balance of power, national technology and industrial bases, and beyond.

---

[7] Gregory Shaffer, *Trade Law in A Data-Driven Economy: The Need for Modesty and Resilience*, 20 WORLD TRADE REVIEW 259, 259-260 (2021).

[8] Susan A Aaronson, *Data Is Different—Why the World Needs a New Approach to Governing Cross-Border Data Flows*, CIGI PAPERS NO. 197 (November 2018), at 2, https://www.cigionline.org/sites/default/files/documents/paper%20no.197_0.pdf.

[9] KAI-FU LEE, AI, SUPERPOWERS: CHINA, SILICON VALLEY AND NEW WORLD ORDER ch.1 (2018).

[10] Kevin Casey, *How Big Data and AI Work Together*, THE ENTERPRISES PROJECT (October 14, 2019), https://enterprisersproject.com/article/2019/10/how-big-data-and-ai-work-together.

[11] Andrew Ng & Michael Chui, *How Artificial Intelligence and Data Add Value to Businesses*, MCKINSEY GLOBAL INSTITUTE (March 26, 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/how-artificial-intelligence-and-data-add-value-to-businesses.

(B) Data Is Different

While the metaphor of oil is apt to describe data's economic value and strategic importance, data is starkly different from oil in many important aspects. Different from fossil fuels, data is by no means in short supply, but rather has almost infinite volumes. As more of our daily life and businesses move into the digital realm, data grows at an ever-accelerating rate.[12] Rather than a single-use, depletable commodity, data is super-abundant, infinitely durable, and recyclable.[13] Notably, data could be reused and combined for new purposes, and often becomes more useful the more it is used.[14] In particular, data exhaust from a specific transaction could be complied into "big data", thus unleashing new potential uses.[15] Unlike oil, the use of data is non-rivalrous in nature, making it possible for different users to simultaneously process and exploit the same data.[16]

Further, distinct from oil, gas, or minerals that travel in physical pipelines, the ways data travels in cyberspace are often borderless, instantaneous, and unterritorial.[17] While data moves around the globe in a primarily borderless medium, the governments that seek to regulate such data exercise their powers primarily within the confines of their territories and jurisdiction, whether through domestic laws, international treaties, or regional regulations. As such, the dichotomy between the unterritorial ways in which data travels and the territorial-based control of states generates increasing regulatory contentions among different governmental actors, increasingly blurring "the line between what is territorial and what is extraterritorial in the regulation of a predominantly unterritorial medium".[18] This makes the regulation of data substantially different from that of conventional commerce, capital, property, and financing that are much more susceptible to states' territorial-based control.[19]

---

[12] Bernard Marr, *Here's Why Data Is Not the New Oil*, FORBES (March 5, 2018), https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#6bb86c1b3aa9

[13] *Id*.

[14] *Id*.

[15] Emanuel Valdés, *What is Data Exhaust and How to Use It for Business*, CIENCE (January 24, 2023), https://www.cience.com/blog/what-is-data-exhaust-in-sales (noting that "[d]ata exhaust can be understood as the result of every single online action deployed by a user. Also known as a data trail, some data exhaust examples include log files, cookies, temporary fields, and every stored information for every digital transaction. This data can create quite a rich user profile, making it extremely important to researchers, marketers, and businesses in general," and that "[b]ig data refers to data sets that are too vast, fast, and complex for the traditional data processing software…. Big data has been already adjusted into a specific correlation with a core function of a business while data exhaust is every other data footprint that was created as a result of all online activity."); *Data Exhaust*, TECHOPEDIA ("Data exhaust refers to the data generated as trails or information byproducts resulting from all digital or online activities…. Data exhaust is widely used in data mining and big data analytics").

[16] Joshua New, *Why Do People Still Think Data Is the New Oil?*, CENTER FOR DATA INNOVATION (January 16, 2018), https://www.datainnovation.org/2018/01/why-do-people-still-think-data-is-the-new-oil/.

[17] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STANFORD L. R. 1193, 1285 (1998) ("Cyberspace's essence is the processing of information in ways and at speeds unimaginable just years ago."). See Lazaro Gamio, *How Data Travels Across the Internet*, WASHINGTON POST (March 31, 2015), https://www.washingtonpost.com/graphics/national/security-of-the-Internet/bgp/ ("Information is divided up, sent in chunks across the world and reassembled when it reaches its destination").

[18] Daskal, *supra*, 181.

[19] Milton Muller & Karl Grindal, *Data Flows and the Digital Economy: Information as A Mobile Factor of Production*, 21 DIGITAL POLICY, REGULATION AND GOVERNANCE 71, 72 (2019) (noting that although territorial control over information flows is increasing, transnational data transfers are "less constrained by national borders than almost any other form of exchange", including capital, physical goods and labor).

Among different categories of data, personal data stands out for its growing prominence and unique characteristics. Today, given the widespread usage of the Internet and the Internet-of-Things, virtually all of our daily life activities generate large quantities of personal data for technology firms to collect, process, transfer, and commercialize, and much of the data flowing across national borders is personal data.[20] Given its enormous economic value, personal data emerges as "a new asset class" and "a critical source of innovation and value", "generating a new wave of opportunity for economic and societal value creation."[21]

Moreover, the access and control of personal data could generate profound adverse effects, endangering individuals' information privacy and a country's national security. For instance, by illegally harvesting a multitude of Facebook users' social media profiles in aid of targeted political advertisements, Cambridge Analytica may have influenced important domestic political processes, including voting in the 2016 U.S. presidential election and the UK's Brexit referendum.[22] In response, national governments, with increased invocations of national security grounds, have been tightening the scrutiny of foreign digital services providers: for example, Indian banned TikTok and WeChat,[23] Russia blocked LinkedIn,[24] and Germany prohibited U.S.-made interactive dolls that can converse with people through AI and U.S.-based servers.[25]

In short, the hybrid nature of personal data—involving economics, privacy (or human rights), and national security—makes data governance particularly complex and challenging, straddling many important fields, including international trade and investment, information privacy protection, cybersecurity, and national security.

Nevertheless, the rules over how data should be collected, stored, moved, exchanged, and used are just at their infancy, and are undergoing intense contestations. The ways data does or does not travel almost inevitably reflect and implement a vision, or several competing visions, which are

---

[20] Aaronson, *supra* (Data Is Different), 2.

[21] World Economic Forum, *Personal Data: The Emergence of A New Asset Class (2011)*, at 5-6. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Meglena Kuneva, European Consumer Commissioner, commented that "(p)ersonal data is the new oil of the internet and the new currency of the digital world.")

[22] See Adrian Chen, *Cambridge Analytica and Our Lives Inside the Surveillance Machine*, The New Yorker (March 21, 2018), https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine; Jane Mayer, *New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexi*t, The New Yorker (November 17, 2018), https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit.

[23] *India Bans TikTok, WeChat and Dozens More Chinese Apps*, BBC (June 29, 2020), https://www.bbc.com/news/technology-53225720 (India banned these apps for they were prejudicial to India's sovereignty and integrity, defence, national security, and public order).

[24] Nabi Abdullaev, *Why Russia's LinkedIn Ban Is Not About Internet Freedoms*, FORBES (December 8, 2016) https://www.forbes.com/sites/riskmap/2016/12/08/why-russias-linkedin-ban-is-not-about-internet-freedoms/?sh=331d86aaa78e (Russia banned LinkedIn for its refusal to store personal data of Russian users within Russia).

[25] Soraya Nelson, *Germany Bans "My Friend Cayla Doll Over Spying Concerns"*, NPR (February 20, 2017), https://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns (Germany cited concerns that the "digital spyware" installed on the doll could facilitate surveillance over children, systemically collect personal data from them and their parents, secretly transfer those data to a US-based voice recognition company, and is vulnerable to hacking).

constructed in divergent ways and have been promoted by different actors.[26] Different conceptualizations of data often reflect divergent priorities of major actors when regulating data flows, and serve their respective interests and agendas. Meanwhile, distinct rulemaking institutions can privilege different interest groups, influencing the ways in which a specific regulatory approach to data flows takes shape.

Regulation of transnational personal data transfers could significantly shape economic, political, and social conditions within and across national borders. In an era where the digital industrialization has been acting as the main engine for future economic development and technological innovation, the economic, normative, and strategic value of personal data could not be more prominent. With immense distributional effects, competing sets of norms, policies, and practices on *when* and *how* data should travel across borders and on *what* terms help to constitute the rules governing the arteries of e-commerce and the digital economy, while increasingly implicating civil liberties, information privacy, and national security.

B. Three Great Powers Across the Globe

The primary actors surveyed by this study are the world's three economic great powers—the U.S., the EU, and China. In the current era of economic globalization, these actors are three leading economies worldwide, standing in their own league in terms of their domestic markets, populations, trade and investment flows, and GDP.[27] In particular, these great powers figure prominently in transnational data flows and the global digital economy.

The transatlantic economies between the U.S. and the EU are highly integrated, featuring enormous commercial exchanges of goods and services coupled with massive reciprocal investments.[28] With both economies deeply connected to the Internet, transatlantic data flows represent the largest inter-continental data flows worldwide.[29] Nowadays, such data flows increasingly serve as the backbone of the transatlantic economies, underpinning e-commerce, trade in services, manufacturing, marketing, logistics, research and development, and almost all business relations involved.[30]

China is a rising economic power with an increasingly competitive digital industry. It has been the world's largest trading nation in goods since 2013, and is among the top two destination and source countries for foreign direct investment.[31] With 1.04 billion Internet users as of 2022, China has

---

[26] Kieron O'Hara & Wendy Hall, *There Are Now Four Competing Visions of the Internet. How Should They Be Governed*, WORLD ECONOMIC FORUM (March 12, 2019), https://www.weforum.org/agenda/2019/03/there-are-now-four-competing-visions-of-the-Internet/.

[27] See *The World in 2050: Will the Shifting in global Economic Power Continue?*, PWC (February 2015), at 1-4, https://www.pwc.com/gx/en/issues/the-economy/assets/world-in-2050-february-2015.pdf.

[28] *Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES (2016), at 13, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf.

[29] *Id*., 13-14.

[30] *Id*.

[31] *China and the World: Inside the Dynamics of a Changing Relationship*, MCKINSEY GLOBAL INSTITUTE (July 2019), at 1, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside

one of the world's largest domestic digital markets.[32] China's digital economy already hit USD 7.1 trillion in 2021, accounting for 39.8% of its annual GDP.[33] These aspects make cross-border data flows in and out of China all the more important for global tech behemoths and small-and-medium firms alike. Overall, the U.S., the EU, and China occupy central positions in global data flows.

C. The Global Regulatory Arena for Great Powers

The emerging field of transnational personal data flows is essentially a regulatory arena where different great powers pursue different transnational rules that reflect their values and serve their interests.

In this regulatory battlefield, the processes of transnational rule-making and global governance are often fused with power asymmetries that great powers states are ready to exploit, with the aim of tilting the balance to their favor. Far from being uncontested, the TPDF system is witnessing a legal and regulatory battle between great powers. Aimed at achieving regional or global dominance, great powers strive to shape the lawmaking initiatives in ways that advance their preferences, interests, and agendas. What is at stake is far more than abstract legal rights and innocuous information, but rather a fledging global networked structure of commerce, privacy, and security that may profoundly (re)shape each country's economic welfare, normative goals, strategic security, and balance of power.

With fertile grounds for scholarly theorization and contestation, this field makes for a good testing ground to explore the relationship between great powers and international law, the behavior of powerful sovereign actors in global economic governance, power politics in competitive regulatory competition, and transnational lawmaking in geo-economic rivalry.

E. How is the Emerging TPDF Framework Different?

In contrast with many other sub-fields of international law, the emerging legal and regulatory framework governing transnational personal data flows ("TPDF framework") manifests distinctive features.

Different from other sub-sectors of international law having a central controlling institution or a multilateral treaty, the TPDF framework did not emerge from an overarching constitutional institution that carefully crafted the essence of this system.[34] At the international level, there is no

---

%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx.

[32] Lai Lin Thomala, *Number of Internet Users in China From 2018 to 2022 with a Forecast until 2027 (in Millions)*, STATISTA (December 9, 2022), https://www.statista.com/statistics/278417/number-of-internet-users-in-china/ ("China is home to the largest online community in the world. According to estimates, the Chinese internet population was around 1.04 billion in 2022…. The country's internet penetration rate is around 72 percent, indicating that almost one out of three Chinese are still offline.").

[33] *China's Digital Economy Hits &7.1T: White Paper*, STATE COUNCIL OF THE PRC (July 30, 2022), http://english.www.gov.cn/archive/statistics/202207/30/content_WS62e515e6c6d02e533532eb06.html.

[34] Joost Pauwelyn, *At the Edge of Chaos? Foreign Investment Law as a Complex Adaptive System, How It Emerged and How It Can Be Reformed*, 29 ICSID REVIEW 372, 378 (2014).

single, integrated international regime governing this issue-area or coordinating the decision-making processes, due to the variety of the regulatory rules, the diversity of the institutions that enacted and enforce such rules, and the failure to agree on a harmonized global standard of privacy protection for cross-border data flows. Rather, the development of the TPDF framework has resulted in considerable legal fragmentations, featuring different regulatory rules, institutions, and governance models vying to dominate the governance of this issue-area.[35]

Instead of having a global hierarchical controller to make rules on data flows in a centralized, multilateral, top-down fashion, the formation of the TPDF framework emerged through numerous self-organizing, multi-layered, organic processes of incremental events. The TPDF framework largely emerged through gradual and continuous "evolution" and "adaptation", rather than a revolutionary process creating overarching constitutional instruments. These processes involve dispersed interactions of different actors that gradually evolved, adapted, and changed over time. While nation-states, international governmental organizations, NGOs, human rights activists, advocacy groups, and academics all participate in the regulatory contestations, three great powers (along with their agents, representatives, organs, and allies) are the most dominant actors in the lawmaking processes, by virtue of their unparalleled power resources and sovereign status.[36]

Importantly, the lawmaking processes that govern TPDF are constantly evolving. In this regard, notable examples include different versions of U.S.-led Preferential Trade Agreements (PTAs) (from the U.S.-Korea PTA to Trans-Pacific Partnership to United States-Mexico-Canada agreement), regional data protection regulations (from the EU Data Protection Directive 1995 to General Data Protection Regulation (GDPR) 2016), transatlantic data flows agreements (from the EU-U.S. Safe Harbor agreement 1995 to Privacy Shield agreement 2018, and then to its successor(s)), domestic legislations on data privacy or national security (such as China's Cybersecurity Law 2016, Personal Information Protection Law 2021, and their implementation regulations), regional and domestic judicial making (e.g., *Schrems I* 2015 and *Schrems II* 2020 of the European Court of Justice (ECJ)). The continuous evolution and adaption processes occur due to the constant interactions among distinct actors in response to policy challenges from the broader environment.[37]

Oftentimes, such dynamic rulemaking processes are driven by multiple sovereign, sub-national, supranational, and non-state actors in pursuit of their prioritized interests. Far from being value neutral, the competing visions over data governance in the global regulatory arena are typically laden with values, interests, and distributive effects, molding the ways in which the global TPDF framework takes shape. Particularly, the institutional architecture governing TPDF has been substantially shaped by powerful governments—most notably, the U.S., the EU, and China—such that the questions of transnational data governance are largely characterized by clashes of the competing visions and approaches of these great powers.[38]

On the other hand, third countries (particularly developing states) often choose to accede to different regulatory rules that are made, applied, and promoted by the Big Three—whether by

[35] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAWS 26 (2011).
[36] See DANIEL W. DREZNER, ALL POLITICS IS GLOBAL 34 (2008).
[37] See Pauwelyn, *supra* (At the Edge of Chaos), 385.
[38] See *infra* chapter 1 ("A Battle of the Big Three").

concluding international agreements or enacting/amending domestic laws—in the hope of facilitating trade/investment flows, nurturing domestic firms and industries, pursuing normative values, or safeguarding strategic interests.[39] In some cases, third states are left struggling about which model to follow over others, creating tensions, conflicts, and fragmentations in the global regulatory environment. And sometimes, these countries are following more than one regulatory approach, generating complex obligations, crisscrossing rules, and inconsistent practices.

II. CORE RESEARCH QUESTIONS

Given the foregoing aspects discussed in the previous section, this research project primarily focuses on the regulation of transnational personal data transfers by the Big Three. Through comparative case studies of these great powers' lawmaking processes, the research strives to explore the conceptualizations, interests (or values), and rulemaking strategies underlying the Big Three's approaches, explain their divergences and commonalities, and discuss their implications for transnational data governance.

At the core, this study aims to develop an analytic framework to explain the lawmaking processes of the U.S., the EU, and China with respect to cross-border personal data transfers for commercial purposes. Specifically, it focuses on three major research questions.

First, what are the Big Three's dominant conceptualizations of personal data regarding this issue-area, and in what ways do they relate to their primary regulatory approaches?

Second, why do these great powers subscribe to divergent conceptualizations of personal data? Specifically, which interests, values, and institutions are driving these great powers to adopt different approaches to regulating transnational data flows? And how are the Big Three deploying competitive lawmaking strategies to shape the rulemaking processes in order to achieve their distinct priorities?

Third, in the global regulatory arena, how are the Big Three's approaches spreading among other follower countries, shaping the latter's data governance approaches in the making? In particular, how are the U.S., the EU, and China getting third countries on board with their regulatory approaches, pushing for their visions, norms, and policies at the international level?

While the second research question delves into the lawmaking processes that created three primary regulatory approaches, the third question explores how each of them is diffusing in the international regulatory arena and influencing a third country's norms—whether through a great power's norm promotion efforts, the ideational power of the norms themselves, or otherwise. Although this thesis takes a holistic approach to examine all major mechanisms of influence, its analysis focuses on the Big Three's norm promotion initiatives, which are arguably the dominant force driving the norm diffusion processes.

[39] See *infra* chapter 2 ("U.S.-led Regime- and Forum-Shifting"), Section III.D; chapter 4 ("Implications of EU Data Protection Law"), Section II; chapter 6 ("Policy Diffusion of the Chinese Approach").

III. THEORIES AND METHODS

To address major research questions laid out in the previous section, this thesis engages with discursive analysis, international relations (IR) theories of regime- and forum-shifting, and select strands of policy diffusion theory. This section briefly presents key theoretical framings of this thesis, as well as the empirical sources used to build its arguments and to apply these theories to the field of TPDF regulation.

A. Discursive Analysis

Regarding the first research question, this project uses discursive analysis to clarify the basic logics of the Big Three's conceptualizations of personal data, revealing divergent benchmarks to determine the major policy goals for regulatory interventions. Specifically, it analyzes how—through competing discourses—different conceptual framings of personal data can influence the normative foundations of transnational data regulation, and help to determine the optimal balance to be struck among distinct interests underlying data flows as a baseline position.

As defined by Michael Foucault, "discourse" is a system that governs the formation of knowledge: it predetermines the objects of knowledge, concepts, theoretical options and the rules of their production.[40] The use of language to frame thoughts and produce knowledge is typically situated in a particular discourse, which implicitly "defines the meaning of terms according to shared practice in line with ideologies of the social groups controlling the discourse."[41] Notably, discourse has the power to "*mediate* the dominant view of what constitutes normality or deviance" and can "'produce' behaviour that is in conformity with the dominant standard of normality or acceptability."[42] In this way, "control over discourse ultimately translates into control over the production of 'truth' at a particular point in time, and allows to suppress the views outside of the prevailing discourse."[43]

In the regulatory context, Julia Black has argued that discourse can constitute the basis of regulation in important aspects: discourse can define the problem, determine the goals that regulation seeks to achieve, and "(produce) shared meanings as to the regulatory norms and social practices which then form the basis for action (for example, the formation of regulatory interpretive communities)."[44] Therefore, states often deploy discursive power to promote their preferred narratives and approaches in international policy debates, shaping the rule-making in the global regulatory arena based on their preferences.[45]

---

[40] MICHAEL FOUCAULT, THE ARCHEOLOGY OF KNOWLEDGE AND THE DISCOURSE OF LANGUAGE 72 (1972). See Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416, 423-24 (2020); See also Julia Black, *Regulatory Conversations*, 29 J. L. & SOC'Y 163, 168 (2002).
[41] Yakovleva, *supra*, 424. See Teun A. Van Dijk, *Ideology and Discourse Analysis*, 11 J. POL. IDEOLOGIES 115, 138 (2006).
[42] Ivan Manokha, *Foucault's Concept of Power and the Global Discourse of Human Rights*, 23 GLOBAL SOC'Y 429, 430 (2009).
[43] Yakovleva, *supra*, 424.
[44] Black, *supra*, 165, 178, 188.
[45] Yakovleva, *supra*, 425.

Although data is subject to different conceptual framings for different purposes,[46] when it comes to cross-border personal data flows for commercial purposes, three primary (yet not mutually exclusive) conceptualizations figure prominently in the discourses of transnational data governance—namely, as an intangible factor of production, an embodiment of fundamental rights, and an element of national security.[47] While a state often balances multiple interests when conceptualizing personal data, these three primary conceptualizations are common to many countries,[48] and are largely predominant in the Big Three's TPDF policymaking.

While a state's conceptualization may evolve over time to respond to changed circumstances, the government often subscribes to a dominant conceptual framing of personal data when designing its primary regulatory approach to cross-border personal data flows at a given time, such that it is possible to make some generalizations regarding different countries' major conceptualizations.[49] This thesis argues that the Big Three, based on their respective dominant *conceptualizations* of personal data, advance divergent discourses that prioritize different interests and values under disparate rationales. As such, different discourses reveal the Big Three's divergent framings of what personal data is and what the TPDF system should be, and can generate normative implications in terms of what policy is deemed legitimate or pathological, thereby influencing the balance struck among economics, privacy, and national security interests underlying data flows.

Further, divergent conceptualizations of personal data suggest different legal *paradigms* to institutionalize their basic logics and policy choices. By "paradigm", I refer to a particular legal

---

[46] See e.g., Jannice Käll, *The Materiality of Data as Property*, 61 HARV. INT'L L. J. FRONTIERS 1 (2020) (discussing the framing of data as property); Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L. J. 513, 515 (2013) (treating personal data as an intangible property of an individual data subject, this work conceptualizes the GDPR as a "property-rights-based approach" to data privacy protection); Kean Birch et al., *Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech,* 8(1) BIG DATA & SOCIETY 1 (2021) (analyzing U.S. "Big Tech" firms' transformation of their users' personal data into an intangible asset that is "measurable and legible as future revenue streams"); Carol Corrado et al., *Data, Intangible Capital, and Productivity*, Paper prepared for the NBER/CRIW Conference on Technology, Productivity, and Economic Growth (March 2022), https://www.imf.org/-/media/Files/News/Seminars/2022/10th-stats-forum/session-iv-corrado-imf-updated-presentation.ashx (conceptualizing data as an intangible asset for industry-level analysis); Travis Toemoe et al., *Touch the Edge—Is Data "Tangible Property" for the Purpose of Your Insurance Policy*, KING & WOOD MALLESONS INSIGHT (March 2017), https://www.kwm.com/global/en/insights/latest-thinking/data-tangible-property-insurance-policy-damage-loss-cover.html; *Should "Data" be Recognised as an Asset on the Balance Sheet?*, ACUTUS (July 31, 2019), https://www.acutus-ca.com/2019/07/31/should-data-be-recognised-as-an-asset-on-the-balance-sheet/ (discussing the viability of treating data as an intangible asset on a company's balance sheet alongside other widely accepted non-physical assets (such as intellectual property, customers list, brand names and logo) under the accounting rules).

[47] See *infra* chapter 1 ("A Battle of Big Three"), section II.

[48] Martina Francesca Ferracane & Erik van der Marel, *Regulating Personal Data: Data Models and Digital Services Trade*, WORLD BANK GROUP (March 2021), World Development Report 2021 Policy Research Working Paper 9596, 5-7, https://openknowledge.worldbank.org/handle/10986/35308 (cataloguing three common data governance models that regulate cross-border data transfers and domestic data processing among various countries). Each model is built on one of the three primary conceptualizations of personal data identified above.

[49] To be clear, for the Big Three, these conceptualizations of personal data and regulatory approaches to cross-border data flows are not static, but rather may be subject to recalibrations, adaptations, and changes over time. For a discussion on how these three great powers adapt their conceptualizations and recalibrate their approaches to manage shifting interests and to accommodate each other, see *infra* chapter 1 ("A Battle of the Big Three"), section IV. Due to my limited space, I leave the broader question of how the Big Three's framings and approaches might change in the future outside the purvey of this project.

field with a shared legal language, a common set of concepts, legal sources, argumentation, and methodology, and a common ideology (i.e., a shared basic world view).[50] Built on different primary conceptualizations of personal data, three major legal paradigms compete to regulate cross-border personal data flows: a trade paradigm, a privacy paradigm, and a security paradigm. Aligned with its major conceptual framing of personal data, a great power often embraces a particular paradigm as its dominant regulatory approach to govern the issue-area of TPDF.[51] These paradigms strive to provide legal and regulatory solutions (including legal prescriptions and enforcement tools) to address the salient problems identified and framed by different conceptualizations of personal data. From this perspective, what is behind the Big Three's divergent conceptualizations of personal data are an array of competing data governance models, differing in their normative justifications, primary policy concerns, substantive rules, and regulatory institutions.

B. International Relations Theories of Regime- and Forum-Shifting

Drawing on international relations (IR) scholarship on the analysis of regime complexity, this study aims to explore the lawmaking strategies deployed by the U.S., the EU, and China to push for their preferred rules to govern cross-border data flows, revealing salient political economy dynamics shaping legal and regulatory outcomes.

According to this analytical lens, a regime complex consists of an array of partially overlapping, nonhierarchical regimes and institutions, competing to lay an authoritative claim to govern a particular issue-area.[52] Different from a single, decomposable international regime, a regime complex is often characterized by several parallel clusters of international agreements, regional regulations, and domestic laws, each hosting different sets of rules and decision-making processes. Whether functionally- or territorially- defined, these agreements, instruments, and institutions create and implement different rules at disparate venues with the participation of distinct actors.[53] And there is no central, hierarchical institution for resolving conflicts between these rules, making it harder to determine where the appropriate authority over an issue-area resides.[54]

Notably, the presence of regime complexity enables a competitive lawmaking strategy of "regime-" and "forum-shifting".[55] Unlike *ad hoc* initiatives to obtain a single favorable decision (often known as "forum shopping"), "regime-shifting" entails "an iterative, longer-term strategy that

---

[50] Mark Van Hoecke & Mark Warrington, *Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative La*w, 47 INT'L & COMP. L.Q. 495, 513-515 (1998); Anthea Roberts, *Clash of Paradigms: Actors and Analogies Shaping the Investment Treaty System*, 107 AM. J. INT'L L. 45, 46-47 (2013).

[51] This is so, even though a great power may also draw on another paradigm to manage its shifting interests and accommodate its relationship with other countries. See *infra* chapter 1 ("A Battle of Big Three"), section IV; *infra* chapter 7 ("Concluding Remarks"), section I.B.

[52] Karen J. Alter & Kal Raustiala, *The Rise of International Regime Complexity*, 14 ANNUAL REVIEW OF LAW AND SOCIAL SCIENCES 329, 334 (2018); Kal Raustiala & David G. Victor, *The Regime Complex for Plant Genetic Resources,* 58 INT'L ORG. 277, 278-279 (2004).

[53] Raustiala & Victor, *supra* (Plant Genetic Resources 2004), 279.

[54] *Id.*; Karen J. Alter & Sophie Meunier, *The Politics of International Regime Complexity*, 7(1) PERSPECTIVES ON POLITICS 13, 13 (2009).

[55] Lawrence R. Helfer, *Regime Shifting in the International Intellectual Property System*, 7(1) PERSPECTIVES ON POLITICS 39, 40 (2009).

seeks to create outcomes that have feedback effects in other venues".[56] Within the structure of a regime complex, there are often multiple venues within and across different institutions, featuring differing mandates, priorities, memberships, entrance barriers, and issue-linkages. Different actors—including nation-states, sub-state, supranational, and non-state actors—may seek to relocate the rule-making processes from one forum to another, in search of a venue that best serves their interests and agendas.[57] While all actors might attempt to do so to pursue their respective agendas, powerful actors (such as a great power) often "have the greatest success employing this tactic", by virtue of their asymmetrical power resources at disposal (such as market power, coercion, law enforcement power, delegated regulatory authority, regulatory capacity, judicial power, legislative authority, and agenda-setting power).[58]

Depending on the demarcation of the relative boundaries, regime-shifting within a regime complex can take three major forms. The first is "forum-shifting" (also known as "*intra-regime* shifting"), which relocates the law-making process from one venue to another located within a single international regime.[59] The second is "horizontal regime-shifting" (i.e., "*inter-regime* shifting"), concerning a shift of rulemaking initiatives to a forum situated in an entirely different regime.[60] Third, where international negotiations are unable to accommodate incompatible preferences, a powerful sovereign actor may resort to its domestic institutions (or, in the case of the EU, the Union's unilateral legislation at a regional level) to forge the governing rules based on its policy preferences.[61] And an actor may pursue regime-shifting in multiple institutions, "moving back and forth between venues seriatim or pursuing parallel lawmaking agendas simultaneously".[62]

At the core, this thesis argues that the existing TPDF system can be conceptualized as a transnational regime complex. Originating from Europe in the 1970s, various TPDF regulations have been increasingly spreading around the globe,[63] and different types of rules have grown substantially over time. These include international trade agreements, international and regional instruments of data privacy protection (whether as international treaties or soft law norms), national laws and regulations (including domestic data privacy laws, trade law institutions, and security-oriented regulations), as well as private-sector self-regulatory mechanisms (such as the APEC Cross-Border Privacy Rules). Absent an overarching multilateral institution to govern

---

[56] *Id.*, 39.
[57] Raustiala & Victor, *supra* (Plant Genetic Resources 2004), 299.
[58] DREZNER, *supra*, 63-64, 67. In domestic policymaking and international bargaining, the reason why these actors are able to impose their preferences on others and achieve their desired policy outcome is usually because they can leverage their power resources to change the "reversion point", thus altering the regulatory status quo that would exist for key policymakers in the absence of their desired policy change. For a discussion of "reversion point", see John E. Richards, *Toward a Positive Theory of International Institutions: Regulating International Aviation Markets*, 53(1) INT'L ORGAN. 1, 13 (1999) ("The reversion point is the set of marketplace rules that will result if there is no new international agreement; absent agreement, the market will 'revert' to some other outcome. When states bargain over the creation of international institutions, they necessarily do so in the shadow of this reversion point.").
[59] Lawrence R. Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking,* 29 YALE J. INT'L L. 1, 16 (2004).
[60] *Id.*
[61] See e.g., HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWERS chapter 5 (2019) (discussing a coalition of privacy-oriented actors' efforts to leverage domestic political/legal institutions to undermine the U.S.-EU Safe Harbor agreement (that allowed unrestricted transatlantic personal data transfers) and to insulate their domestic privacy systems from transnational pressures).
[62] Helfer, *supra* (TRIPs 2004), 14 (fn 51).
[63] KUNER, *supra* (TRANSBORDER DATA FLOWS 2011), 25.

cross-border data flows, the key principles, norms, and rules are increasingly developed and enforced through several clusters of sometimes competing and partially overlapping international regimes and regional/domestic institutions, resulting in increasing crisscrossing rules, complex obligations, and legal fragmentations.

In this context, the expansion of TPDF rulemaking processes into parallel international, regional, and domestic institutions and venues often embodies the lawmaking strategy of "regime-" and "forum-shifting". Dissatisfied with the multilateral rulemaking stalemate, the U.S., the EU, and China have been striving to create, develop, and recalibrate their preferred approaches at alternative institutions and fora, in pursuit of their own visions, interests, and agendas. Depending on the distribution of interests and power politics of different institutions, the Big Three strategically move the decision-making processes over an issue-area from one forum to another, abandon a particular venue (or threaten to do so), and pursue the same agenda in multiple fora back and forth, so as to magnify their power in shaping the legal and regulatory outcomes. As such, different regimes and institutions where contentious lawmaking processes take place reflect a regulatory battle among these great powers, racing to make rules that reflect their visions and serve their policy preferences.

C. Policy Diffusion Theory

In response to the third research question, this thesis draws on policy diffusion theory from IR studies to distill key mechanisms, seeking to explain the incentives and interests animating the spread of a given regulatory approach from one jurisdiction to another.

In IR literature, there are four widely accepted policy diffusion mechanisms: coercion, competition, imitation, and learning.[64] Defined in a broad sense, "coercion" refers to the use of political, economic, or other coercive power to force weaker actors to adopt or change their policies and practices.[65] For example, a powerful state may condition access to its large market on the adoption of a specific policy, or sanction foreign firms or governments breaching its regulatory rules. During bilateral negotiations, a great power can also use issue-linkage to set conditions for a small country reliant on its trade flows, foreign direct investments, financial aid, grants, or loans.[66] More generally, coercion may function via the market mechanism, conferring a government with the unilateral power to regulate the global market.

With strong gravitational effect, a state's large market could generate significant economic incentives for foreign firms to mirror its preferences and regulatory standards, in order to secure their market access.[67] The greater the market, the stronger the pull. Notably, a government with a sufficiently large market can use the market mechanism to change the incentives of foreign private actors, which then may lobby and pressure their governments to alter the relevant economic

[64] See eg., Beth A Simmons, Frank Dobbin, and Geoffrey Garrett, *Introduction: The International Diffusion of Liberalism*, 60(4) INT'L ORG. 781, 781 (2006).
[65] Frank Dobbin, Beth A. Simmons, and Geoffrey Garrett, *The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning*, 33 ANNUAL REVIEW OF SOCIOLOGY 449, 454 (2007).
[66] *Id.*
[67] DREZNER, *supra*, 34.

policies.[68] By virtue of this mechanism, an economic power has less incentive to switch its regulatory standards; rather, its standards often serve as an attractor for profit-seekers, causing other actors (private or public) to converge to its preferences.[69]

In this regard, the best known example is the "Brussels Effect" theorized by Anu Braford, referring to the scenario where the EU is empowered to externalize its regulatory standards globally by unilaterally regulating the European market.[70] According to Braford, five elements are required for the Brussels effect to take place: (i) a large market, (ii) strong regulatory capacity, (iii) stringent regulatory standards, (iv) inelastic targets (i.e., the subject matter of regulation), and (v) non-divisibility (i.e., it is not legally, economically, or technically feasible for a firm to tailor standards in different markets).[71]

Under the "competition" mechanism, states compete with their peers and adopt policies to pursue expected economic benefits.[72] Under peer pressure, a state may have little choice but to embrace certain policies to compete for export markets or foreign capital flows, when their direct competitors have already done so.[73] For instance, if a developing country adopts a given market-friendly policy to attract foreign investment, its neighboring countries may be pressured to follow suit, for fear that the first-mover would seize a lion's share of capital flowing to the region.[74]

"Imitation" refers to the scenario where a state is drawn to the policies of a perceived exemplar country, due to its trust in the latter as a successful model.[75] Given that pursuing policy innovations is often time-consuming and costly, mimicking the policies of a "role model" state can offer an efficient option, especially for countries lacking regulatory expertise or financial resources to comprehensively evaluate different policies.[76] By virtue of this mechanism, later-comer countries may imitate the policies of a key forerunner state that is highly reputed as a successful regulator.[77]

Finally, "learning" is a socialization process where a regulator carefully considers its country's needs and learns a regulatory innovation from foreign regulators, due to the normative appeal of the substantive rules or regulatory design.[78] In addition, when addressing similar regulatory challenges, regulators are often inclined to adopt similar policies and learn from the experiences of other countries with a shared identity, which may derive from geographic proximity, similarity of development status, ideology, regulatory systems, or historical/cultural ties.[79]

---

[68] Scott James & David Lake, *The Second Face of Hegemony: Britain Repeal of the Corn Laws and American Walker Tariff of 1846*, 43 INT'L ORG. 1, 4, 6-8 (1989) (noting that in this process, the government utilizes its market power to alter the constellation of interests and political power in foreign countries in ways more aligned with its own interests). See DREZNER, *supra*, 34.
[69] DREZNER, *supra*, 32-33.
[70] ANU BRAFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 25-26 (2020).
[71] *Id.* For a detailed discussion, see *infra* Chapter ("Implications of EU Data Protection Law"), Section II.B.-C.
[72] Dobbin, Simmons, and Garrett, *supra*, 457.
[73] *Id.*
[74] *Id.*, 457-8.
[75] Cheng-Yun Tsang & Ping-Kuei Chen, *Understanding Policy Diffusion Mechanism of Financial Regulatory Innovation*, 30 ASIA PACIFIC LAW REVIEW 21, 30 (2022).
[76] *Id.*
[77] *Id.*, 30-1.
[78] *Id.*, 29.
[79] *Id.*, 30.

Either individually or in combination, these mechanisms function to change the incentives of other countries, pushing and pulling them to embrace the policies of a major power. This thesis draws on these analytical lenses, and applies them to the case of cross-border data flows. It argues that the Big Three have been strategically deploying these mechanisms (though adapted to suit different contexts) to spread their regulatory approaches at the international level, attracting third countries to sign up to their preferred rules. As a result, three primary (though not mutually exclusive) regulatory "spheres of influence" are in the making over time, empowering these great powers to set the regulatory standards in the global regulatory arena.

D. Empirical Sources

This thesis draws on a wide array of primary and secondary sources of empirical inputs to examine the Big Three's TPDF lawmaking initiatives. By "primary sources", I refer to international trade and investment treaties, regional data protection regulations and instruments (e.g., the GDPR, OECD Guidelines, Convention 108), transatlantic data transfers agreements (i.e., the EU-U.S. Safe Harbor and Privacy Shield agreements), domestic laws on data privacy, consumer protection, and cybersecurity, and judicial decisions of supranational courts and tribunals (such as the ECJ and European Court of Human Rights). By "secondary sources", I am talking about scholarly literature, research studies, and policy reports issued by governments, international organizations (such as the OECD), think tanks, and NGOs, historical archives, media accounts, as well as statements made by key figures of public authorities (eg., the United States Trade Representative (USTR), European Commission, Cyberspace Administration of China (CAC)).

Given the breadth of my research questions and the limited timespan and funding of this project, I did not conduct interviews to collect empirical input, but instead relied on a desk research to examine existing primary and secondary sources.[80] In that regard, two other pragmatic considerations also account for this approach. The first is the measures of border closure and travel bans implemented by many countries (especially China) during the COVID-19, making on-site interviews burdensome and costly (if not impossible). Second, in light of China's not-so-transparent legislative and regulatory processes, it is difficult for scholars and PHD students to carry out on-site interviews with important Chinese officials, legislators, and policymakers. Yet, I have relied on various secondary data where it is available in academic literature, policy reports, or think tanks' studies. Due to my language skills with Mandarin, I am also able to access many Chinese-language sources that are not currently available in English—such as national laws and regulations, the Chinese government and Communist Party's policy instruments, Chinese political leaders' speeches and statements, the authorities' press releases, media reports, Chinese scholarship, and commentaries.

IV. CONTRIBUTIONS TO THE EXISTING LITERATURE

[80] My concern is that if I primarily rely on interviews to obtain empirical data, I may have to apply this approach consistently with respect to the U.S., the EU, and China. Yet, to do so is not viable for me, given the broad scope of the research project and my limited resources at hand.

As transnational data flows have been gaining increasing prominence in global economic governance, there is a proliferation of legal literature and commentaries studying the regulation of this issue-area over time. This thesis distinguishes itself from many existing works on the following six major aspects, seeking to make its own contributions to the current legal and policy discussions.

First, it utilizes the analytical lens of regime complexity studies to capture the systemic nature of the rules and institutions that three great powers have created through their respective lawmaking processes, revealing the essential common elements of the mass of different international, regional, and domestic legal sources regulating TPDF.[81] While there is no shortage of legal and policy analyses of the emerging TPDF framework, much of existing scholarship tends to focus on a particular part of the underlying system. Typical examples include the application and reform of the WTO agreements,[82] digital trade rules of U.S.-led and/or EU-led PTAs,[83] the regulation of transborder data flows by data privacy laws (especially European data protection regulation),[84] and domestic laws and regulations that localize data storage and restrict cross-border data flows ("data localization" measures).[85] Despite the importance of these individual studies, it remains

[81] See Jeswald W. Salacuse, *The Emerging Global Regime for Investment*, 51 HARV. INT'L L. J. 427, 435-36 (2010) (describing how regime analysis from IR studies can be used as an analytical framework to review the mass of decentralized international investment treaties).

[82] A salient strand of trade law scholarship focuses on the application of existing WTO rules to regulate cross-border data flows, and seeks to synchronize the multilateral trade agreements and institutions with the rapidly shifting realities of the new digital economy. See e.g., Andrew Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VANDERBILT J. TRANSNAT'L L. 1073 (2018); Andrew Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World*, 22 J. INT'L ECON. L. 389 (2019); Nivedita Sen, *Understanding the Role of the WTO in International Data Flows,* 21 J. INT'L ECON. L. 323 (2018); L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, *in* RESEARCH HANDBOOK ON TRADE IN SERVICES 371 (Pierre Sauvé & Martin Roy eds., 2016).

[83] Through traditional doctrinal analysis, many scholars have mapped out the legal technicalities of important PTA provisions with respect to the regulation of cross-border data flows. Among the trade treaties surveyed, what attracts the most attention tends to be U.S.-led PTAs. See e.g., Mira Burri, *Creating Data Flow Rules through Preferential Trade Agreements*, forthcoming in DATA SOVEREIGNTY ALONG THE DIGITAL SILK ROAD (Anupam Chander & Haochen Sun eds., 2022), https://digitaltradelaw.ch/wp-content/uploads/2022/09/Burri_Creating-Data-Flows-Rules-through-Preferential-Trade-Agreements.pdf; Mira Burri, *The Regulation of Data Flows Through Trade Agreements,* 48 GEO. J. INT'L L. 408 (2017); Thomas Streinz, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, in MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP 330 (BENEDICT KINGSBURY ET AL., EDS., 2019); Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH. 182 (2017); Susan A. Aaronson, *What Are We Talking about When We Talk about Digital Protectionism?*, 18(4) WORLD TRADE REVIEW 541 (2019); Mark Wu, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, ICTSD (November 2017), http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf.

[84] See e.g., KUNER, *supra* (TRANSBORDER DATA FLOWS 2011), 40-49, 64-66, 86; Richard J. Peltz-Steele, *The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation*, 19. J. INTERNET L. 1 (2015); Anupam Chander, *Is Data Localization A Solution for Schrems II?*, 23 J. INT'L ECON. L. 771 (2020); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000); Peter Blume, *Transnational Data Flow: Is There a Solution in Sight?*, 8 INT'L J. L. & INFO. TECH. 65 (2000).

[85] See e.g., Anupam Chander & Uyên P Lê, *Data Nationalism*, 64 EMORY LAW JOURNAL 677 (2015); Anupam Chander & Uyên P Lê, *Breaking the Web: Data Localization vs. The Global Internet*, UC DAVIS LEGAL STUDIES RESEARCH PAPER SERIES, Research Paper No. 378 (April 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858; John Selby, *Data Localization Laws: Trade Barriers*

challenging to figure out what different international, regional, and domestic rules may add up to in the aggregate—unless they are holistically examined to put together different pieces of a puzzle. To fully understand the complexity and dynamics of the emerging TPDF system at a global level, we may have to examine the evolution of, and interactions between, this field's disparate constituent parts,[86] and think about the broader question "[h]ow do we use the information gleaned about the parts to build up a theory of the whole".[87]

In this regard, regime complexity studies can help us to overcome this analytic hurdle, as it allows a holistic view on the systemic nature of what a great power has developed through interactive and iterative lawmaking processes over time. Viewed through this analytical framework, the creation and evolution of the U.S., the EU, and China's primary regulatory approaches are the result of three competing rulemaking processes, which were dominated by the Big Three to shift the decision-making authority over TPDF to a trade paradigm, a privacy paradigm, and a security paradigm, respectively.[88] As such, we can have a systemic understanding of what discrete U.S. PTAs rules, European data protection norms, and Chinese security-oriented measures amount to in the "spaghetti bowl" of crisscrossing TPDF rules, and have a regime-level comparison among competing international, regional, and domestic institutions deployed by three great powers to shape the emerging international standards based on their preferences. Meanwhile, through the lens of regime complexity, we could also think about how different rules advanced by distinct great powers interact with each other in the transnational regime complex governing TPDF, and consider the implications of such divergent rules for the emerging transnational digital order.[89]

Second, this thesis applies the theories of regime- and forum-shifting to analyze how a dominant regulatory approach of a great power comes into shape, capturing the often overlooked insights of how power dynamics may bring in legal and policy change in the global regulatory arena. International lawyers often tend to undertheorize the systemic-level lawmaking strategies adopted by powerful actors (such as the Big Three) to shape the transnational rulemaking processes based on their preferences. To the extent that existing legal scholarship has engaged these theories to explore global lawmaking initiatives, most of these works dealt with other issue-areas, such as

---

or Legitimate Response to Cybersecurity Risks, Or Both?, 25 INT'L J. L. INFO. TECH. 213 (2017); Henry Gao, *Data Regulation with Chinese Characteristics*, in BIG DATA AND GLOBAL TRADE LAW 245 (Mira Burri ed., 2021); Shin-yi Peng & Han-wei Liu, *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?*, 51 JOURNAL OF WORLD TRADE 183 (2017).

[86] Pauwelyn, *supra* (At the Edge of Chaos), 382-83 (noting a catch phrase of many scholars studying the complexity theory: "the whole is more than the sum of its parts").

[87] STUART A KAUFFMAN, AT HOME IN THE UNIVERSE, THE SEARCH FOR LAWS OF SELF-ORGANIZATION AND COMPLEXITY i (1995).

[88] See *infra* chapters 2, 3, and 5. A notable example to these three primary legal paradigms is the U.S.-EU data transfer agreements, which were concluded by two equivalent great powers as a comprise to bridge their divergent internal data privacy regimes and to facilitate transatlantic commerce data transfers from Europe to the American market. Caught between a trade paradigm (that largely relies on business self-regulation) and a privacy paradigm (featuring implementation of European data protection norms), this institutional framework is of a *sui generis* nature, drawing on institutions from the data privacy regimes of both sides to implement European data protection norms. See *infra* chapter 3 ("EU's Forum-Shifting"), section IV; Paul Schwartz, *Global Data Privacy: The EU Way*, 94 NYU L. REV. 771, 796-7, 799 (2019) (noting that the Safe Harbor promoted business self-regulation by "leaving it up to firms to decide whether or not to follow its principles through an opt-in system" and by allowing participating firms "to use third-party private organizations as an element of their oversight of compliance"; and that this agreement's substantive content contained core principles of data privacy protection reflective of European data protection regulation).

[89] See *infra* chapter 7 ("Concluding Remarks"), section IV.

intellectual property rights, international trade, and foreign direct investment.[90] And many of them revolved around the cases of the U.S. and the EU, with China's use of competitive lawmaking strategies relatively understudied.

In other words, existing international law literature has yet to engage the theories of regime- and forum-shifting to systemically study the creation and development of competing regulatory approaches by the Big Three to dominate the governance of TPDF. Yet, the subject matter of cross-border personal data flows provides an important case-study to explore how these competitive lawmaking strategies have been playing out with three great powers in the emerging regime complexity. Unlike strictly doctrinal legal analyses that often yield a relatively static picture of given rules, these theories can allow us to delve into the iterative processes of regime evolution and development, thus bringing to light the fluidity and dynamism of the underlying TPDF system. By engaging such theories as analytical tools, this thesis strives to provide a comprehensive, layered, and nuanced account on why and how the Big Three came to adopt different primary regulatory approaches to govern TPDF.[91]

Third, existing academic works often primarily focus on the data governance approaches of the EU and/or the U.S., as well as the transatlantic institutional arrangements for U.S.-EU data transfers.[92] In contrast, in-depth exploration of China's regulatory approach is relatively scarce. To fill this gap, Chapter 5 of this thesis provides a multi-faceted account on China's newly emerged comprehensive data governance framework, situating its lawmaking processes in the broader political, economic, and institutional context.[93]

To that end, it expounds the apparently vague and confusing notions of "cyber sovereignty" and "data sovereignty"—the overarching normative underpinnings of China's cyberspace governance

---

[90] See e.g., Eyal Benvenisti & George W. Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595 (2007) (detailing the moves led by the U.S. and the EU to shift the multilateral trade lawmaking from the GATT to the WTO at the Uruguay Round negotiations, as well as the negotiations of UNCLOS and international investment treaties where the U.S. deployed "forum-shifting" to effectively reshape the regulatory outcomes based on its preferences); Helfer, *supra* (TRIPs 2004) (discussing the regime- and forum-shifting initiatives deployed by the U.S., the EU, private interest groups, and civil society members to make competing rules for international intellectual property rights (IPR)); Susan K. Sell, *TRIPS Was Never Enough: Vertical Forum Shifting, FTAs, ACTA, and TTP*, 18 J. INTELL. PROP. L. 447 (2011) (documenting the U.S.'s forum-shifting efforts to use bilateral and regional PTAs to continuously ratchet up IPR rules after the TRIPs agreement); Peter Drahos, *Securing the Future of Intellectual Property: Intellectual Property Owners and Their Nodally Coordinated Enforcement Pyramid*, 36 CASE W. RES. J. INT'L L. 53 (2004) (detailing the U.S.'s "forum shopping" initiatives to use bilateral PTAs to set higher standards of IPR protection when encountering resistance on rulemaking at the multilateral TRIPS Council).

[91] See *infra* chapters 2, 3, and 5.

[92] See e.g., Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 115 (2017). See also Paul Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALI. L. R. 877, 877 (2014); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty,* 113 YALE L. J. 1151 (2004); Richard J. Peltz-Steele, *The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation*, 19 J. INTERNET L. 1, 26 (2015); Andrew Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, INT'L ORGAN. 103 (2008); ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008); HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 29 (2019); Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHICAGO L. R. 49 (2023).

[93] See *infra* chapter 5 ("China's Data Sovereignty").

policies—and analyzes the political economy undergirding the Chinese data localization measures.[94] Further, this chapter traces the evolution of the Chinese data governance framework, and provides a comprehensive legal analysis of its regulatory requirements and legal technicalities on cross-border data flows, demonstrating how this legal system diverges from the U.S. and European data governance approaches and how it may impact international businesses.[95] Through the case studies of China's international trade negotiations and its transnational data privacy rulemaking, this chapter also discusses how the Chinese data regulations influence parallel international regimes governing cross-border data flows.[96]

Fourth, this thesis strives to produce a comparative account of the Big Three's TPDF regulatory approaches, delving into their primary conceptualizations of personal data, their competitive lawmaking processes, and how these approaches are diffusing internationally in different ways. Given the lack of in-depth comparative legal scholarship that systematically surveys the data governance frameworks of these three great powers, this thesis makes an original contribution by offering a comprehensive case study on the issue-area of TPDF. In so doing, this project aims to enrich and deepen our understanding about the various complexities and nuances of the regulatory approaches by three great powers.

Fifth, focused on the regulation of cross-border data flows, this thesis seeks to produce a comparative analysis of how three great powers are advancing and diffusing their regulatory approaches at the international level, thus influencing the transnational regulatory environment in ways that align with their preferences and advance their agendas.[97] In the current legal literature on norm diffusion, scholars tend to focus on the role of influential Western regulators as the dominant global regulators or norm entrepreneurs,[98] leaving the case of China relatively under-researched.[99]

With respect to data governance, many works primarily devote their attention to studying how European data protection norms come to increasingly influence other countries' data privacy rulemaking, whether through Brussels' unilateral market power (i.e., the Brussels Effect),[100] the EU's bilateral "adequacy" negotiations with its trade partners, or the ideational power of European

[94] *Id.*, sections I to II.
[95] *Id.*, sections III to V.
[96] *Id.*, section VI.
[97] See *infra* chapters 2 (section V), 4, and 6.
[98] See e.g., DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 6 (1995) (theorizing a "California effect"—a process where "powerful and wealthy 'green' political jurisdictions (successfully) promoting a regulatory 'race to the top' among their trading partners"); Shaffer, *supra* (*Globalization and Social Protection* 2000), 4-8 (analyzing how the EU pressured the U.S. to embrace stricter European data protection rules, thus ratcheting up U.S. data privacy standards); BRAFORD, *supra* (BRUSSELS EFFECT 2020), 25-6; Anu Braford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2015); Schwartz, *supra* (EU Way), 771 (analyzing the mechanisms and factors explaining the diffusion of EU data protection norms as the *de facto* global standards); Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021).
[99] Daniëlle Flonk, *Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control*, 97 INT'L AFFAIRS 1925, 1925 (2021) (noting that the current literature on policy diffusion features "a liberal bias", primarily focused on the spread of norms from liberal states to other countries).
[100] BRAFORD, *supra* (BRUSSELS EFFECT 2020), 142-55; Braford, *supra* (Brussels Effect 2015), 22-26.

norms in global privacy discourses.[101] To the extent that the case of the U.S. was studied, existing scholarship often analyzed how the U.S. was influenced by, or reactively responded to, European data protection law, in efforts to maintain undisrupted transatlantic commercial data exchange.[102] In relative terms, little is known about how the U.S. *proactively* uses international trade policymaking to externalize its domestic data privacy regime (that largely relies on business self-regulation)[103] to its trading partners and beyond—a topic that Chapter 2 of this thesis aims to address.[104]

Recently, there emerged a new strand of scholarship that analyzed the diffusion of the Chinese approach to Internet and data governance abroad.[105] In a leading work, Matthew Erie and Thomas Streinz theorized a "Beijing Effect"—namely, a mix of "push-and-pull" factors that animate the diffusion of China's data governance approach in emerging markets, without the use of coercion.[106] Among these factors, their analysis focused on the oftentimes underappreciated role of Chinese tech firms, whose increasing export of digital infrastructures to emerging markets has facilitated China's growing influence in transnational data governance.[107] As such, the Beijing Effect starkly contrasts with the "hard-law" legal instruments that are often deployed by the U.S. and (to a lesser degree) the EU to impose their data governance approaches on other countries (especially those heavily relying on their markets) through formal legal requirements.[108]

Building on Erie and Streinz's arguments and theoretical framings, Chapter 6 of this thesis further explores these "push-and-pull" factors by emphasizing other specific mechanisms of influence, adding more nuances to the norm diffusion analysis. Specifically, it focuses more closely on the Chinese governments' multifaceted, proactive, and coordinated norm promotion initiatives at the

---

[101] Schwartz, *supra* (EU Way), 818; Shaffer, *supra* (*Globalization and Social Protection* 2000), 39-46.

[102] See e.g., Schwartz, *supra* (EU Way), 793-803 (discussing the U.S. and the EU's negotiations of the Safe Harbor and Privacy Shield agreements); Shaffer, *supra* (*Globalization and Social Protection* 2000), 39-46, 55-80 (analyzing how the implementation of the Safe Harbor agreement had leveled up U.S. data privacy standards); FARRELL & NEWMAN, *supra* (OF PRIVACY AND POWER), 125-159 (detailing the transatlantic initiatives and efforts to establish, maintain, reform, and challenge the Safe Harbor and Privacy Shield arrangements).

[103] See Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STANFORD L. REV. 1315, 1331 (1999).

[104] See *infra* chapter 2 ("U.S.-Led Regime- and Forum-Shifting"), section IV.C.(A)(b)(2) (detailing the U.S.'s efforts to promote the APEC CBPR system at the regional and international level), and V (discussing the diffusion of U.S.-promoted norms).

[105] See e.g., Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 NYU J. INT'L L. POLITICS 1 (2021); Willem Gravett, *Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa*, 20 AFR. HUM. RIGHTS L. J. 125 (2020); Chris Alden & Daniel Large, *On Becoming a Norms Maker: Chinese Foreign Policy, Norms Evolution and the Challenges of Security in Africa*, 221 CHINA QUARTERLY 123 (2015); Flonk, *id.*, 1926 (analyzing the role of China and Russia as norm entrepreneurs internationally, diffusing the norms on Internet content control).

[106] Erie & Streinz, *supra*, 2 ("Governments in emerging economies demand Chinese-built digital infrastructures and emulate China's approach to data governance in pursuit of data sovereignty and digital development. China's 'Digital Silk Road,' a massive effort to build the physical components of digital infrastructure (e.g., fiber-optic cables, antennas, and satellites), to enhance the interoperability of digital ecosystems in such developing states materializes the Beijing Effect. Its main drivers are Chinese technology companies that increasingly provide telecommunication and e-commerce services across the globe.").

[107] *Id.*, 2.

[108] *Id.*, 35-37.

international level, as well as the ideational appeal of the China's approach to like-minded developing countries facing similar policy challenges.[109]

Overall, this thesis engages salient strands of policy diffusion scholarship, and contributes to the current debates by systemically analyzing the case-studies of the U.S., the EU, and China with respect to TPDF. By exploring the mechanisms that serve to pressure and incentivize foreign governments to embrace three great powers' visions, norms, and policies, this project seeks to explain how these great powers are increasingly capable of shaping follower countries' nascent data governance frameworks based on their own preferences.[110] Further, by situating the discussion of norm diffusion in the context of regime complexity, this thesis demonstrates how the Big Three are competing to establish the emerging regulatory standards for TPDF in the transnational regulatory arena.[111]

Sixth, this thesis helps to construct a way of understanding how these dominant regulatory approaches are interacting with each other in a dynamic way, creating a transnational data governance system that is multilayered, complex, fragmented, and constantly evolving. In international legal studies and IR literature, there emerges a growing trend of applying complexity theory to explore intricate, contentious global governance issues (such as the regulation of foreign investment, international trade, environmental protection, and climate change).[112] This thesis joins the discussions by exploring a novel, important, and emerging field—the regulation of cross-border personal data flows—thus providing a concrete case study for the development of a more theoretical framework by subsequent international lawyers and scholars.

In particular, this thesis can help international law scholars to understand how a transnational regime complex shapes, and is in turn shaped by, the lawmaking strategies of different sovereign,

---

[109] See *infra* chapter 6 ("Policy Diffusion of the Chinese Approach"), section III.A. and C.

[110] This thesis argues that the diffusion of these approaches is largely the result of the Big Three's norm promotion efforts, whether through coercive means (such as issue-linkage) or international advocacy. Meanwhile, this process is also due to the perceived attractiveness and ideational power of three primary regulatory approaches, pushing and pulling a third country to come on board with the Big Three's preferred norms. In the case of China, when supplying digital infrastructures and technologies to emerging markets, Chinese tech firms also facilitate the spread of the Chinese regulatory approach abroad, to the extent that their commercial interests overlap with the government's norm promotion agenda.

[111] Among different mechanisms of policy diffusion, a great power's norm promotion is oftentimes a precondition for other factors to come into play, and is arguably the dominant mechanism driving this whole process. Generally, the greater the norm diffusion, the higher the likelihood that a great power can turn its preferred norms into part of the emerging international standards.

[112] For international legal studies, see e.g., Anthea Roberts & Taylor St. John, *Complex Designers and Emergent Design: Reforming the Investment Treaty System*, 116 AM. J. INT'L L. 96 (2022); Pauwelyn, *supra* (At the Edge of Chaos), 375; Sergio Puig, *International Regime Complexity and Economic Law Enforcement*, 17 J. INT'L ECON. L. 491 (2014); Jean Frédéric Morin, Joost Pauwelyn & James Hollway, *The Trade Regime as a Complex Adaptive System: Exploration and Exploitation of Environmental Norms in Trade Agreements*, 20 J. INT'L ECON. L. 365 (2017); Rakhyun E. Kim & Brenda Mackey, *International Environmental Law as a Complex Adaptive System*, 14 INT'L ENVTL. AGMTS.: POL. L. & ECON. 5 (2014). Regarding IR literature, see e.g., Alter & Meunier, *supra* (Politics of Regime Complexity 2009), 13; Alter & Raustiala, *supra* (Rise of Regime Complexity 2018), 329; Kenneth W. Abbott, *The Transnational Regime Complex for Climate Change*, 30 ENV'T & PLAN. C: GOV'T & POL'Y 571 (2012); Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. POL. 7 (2011); Antoine Bousquet & Simon Curtis, *Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations*, 24 CAMBRIDGE REV. INT'L AFF. 44 (2011); Raustiala & Victor, *supra* (Plant Genetic Resources 2004), 278-79.

sub-state, supranational, and non-state actors to advance their preferred rules in pursuit of their preferences. In the current era featuring increasing economic, security, and value competition among multiple powers, this case study can provide a template for international lawyers, academics, and policymakers alike to think about how great powers' regulatory competition can shape transnational rulemaking based on their visions and interests, how power dynamics inherent in lawmaking processes may influence legal and policy outcomes, and how global economic governance could proceed over other contentious issue-areas.

V. CAVEATS OF THE RESEARCH

Broadly speaking, the project is confined in three major aspects. First, as noted earlier, this research adopts a comparative approach to survey the lawmaking processes of three major powers—the U.S., the EU, and China. This means that much of other states' norms, practices, and policies are beyond its purview (other than what is relevant for the third research question), despite that their potential importance.

Second, the core issue-area targeted by this project is the transfers of personal data between different private-sector actors across different jurisdictions for commercial purposes. Though nowadays much of the data transferred across national boundaries is personal data, the latter represents only part of the whole corpus of digitalized information ("data" in the broad sense) traversing the globe. And the broad notion of data governance cuts across numerous fields, including macro-economy, industrial policy, privacy and consumer protection, civil liberties, telecommunication regulation, Internet governance, law enforcement, and national security. But the focus of this project is more narrowly oriented: to capture select interdisciplinary interfaces crucial for and closely related to understanding the regulation of *cross-border personal data transfers*—namely, the legal disciplines of international trade, information privacy, and national security.

Third, the project is primarily concerned with the intersection between transnational data regulation and international economic governance (particularly international trade and investment). It does not focus on national legislations governing law enforcement agencies' extra-territorial access to personal data (such as the U.S. CLOUD Act), or inter-governmental arrangements and instruments to exchange personal data for law enforcement or security purposes, though they are also an important part of the transnational data transfer system.

VI. A ROADMAP OF THE PROJECT

Structurally, this PHD project consists of seven chapters. This section provides a brief overview of the main content of each chapter, clarifies the relationship between different chapters, and situates the specific chapters into the broader research design of this project.

To address the first research question, Chapter 1 unpacks the Big Three's dominant conceptualizations of personal data, and analyzes their normative implications for the (re)design of the emerging legal and regulatory framework governing TPDF. Intended to be transversal across all three case-studies, this chapter provides a static, bird-eye view of the Big Three's primary

regulatory approaches to TPDF, explaining how their major conceptual framings of personal data relate to their data governance models. It also discusses how the Big Three have been increasingly adapting their conceptualizations of personal data and switching their approaches to regulate cross-border data flows, in efforts to balance their shifting interests and to accommodate each other in transnational economic governance.

Chapter 2 to 6 proceed to present three in-depth case-studies of the U.S., the EU, and China. Focused on the second research question, Chapters 2, 3, and 5 explore three lawmaking processes of the U.S., the EU, and China, respectively, charting the institutional trajectory through which their regulatory approaches came into shape.[113] By engaging the theories of regime- and forum-shifting, these three chapters delve into how three great powers have pushed for the governing rules in ways that reflect their visions, serve their preferences, and take advantage of their institutional capacities.

Specifically, Chapter 2 explores the development of a U.S.-led trade-based approach, and traces the lawmaking processes where the USTR deployed international trade agreements to regulate TPDF on its preferred terms. It argues that within the transnational regime complex, the U.S. has leveraged horizontal regime-shifting and vertical forum-shifting to shape the rulemaking processes based on its policy preferences, anchoring and refining the governance of this issue-area in the international trade regime. In particular, through vertical forum-shifting below the multilateral level, the U.S. was able to magnify its market clout and negotiating leverage vis-à-vis its divided trade partners, thus dominating the rulemaking processes. As a result, the U.S. managed to reconfigure international trade law based on its domestic digital trade agenda, while empowering the international trade regime to make a strong claim to govern cross-border data flows.

Chapter 3 studies the EU's lawmaking initiatives to create and develop European data protection regulation. Through the analytical lens of forum-shifting, this chapter provides a different account on the emergence and evolution of EU data protection law. Contrary to conventional wisdom, European data protection regulation is neither preordained by Europe's historical or cultural legacies, nor simply a result imposed by powerful EU members states out of national economic interests. Instead, this chapter argues that this legal regime is the result of contentious lawmaking processes launched to address regulatory challenges and alter existing institutional rules. At the core, it explores how a powerful coalition of privacy-oriented institutional actors in Europe leveraged asymmetrical power resources to impose their policy preferences on the Union level, and deployed forum-shifting to create, develop, and reform European data protection regulation, shaping supranational rulemaking based on their policy preferences.

Chapter 5 explores the evolution and development of China's internal data governance regime. Driven by the intertwined objectives of national security and development goals, China chooses to make its preferred rules through its domestic legislative process (that is much more submissive to Beijing's political will and governmental control than are international institutions), and implements such rules through security-minded authorities' regulatory enforcement, supervision, and monitoring. With the adoption of a comprehensive internal data regulatory framework, China

[113] Though Chapters 2, 3, and 5 may have some overlap with Chapter 1 (which is meant to be transversal across all three case studies), they are more thorough and comprehensive, delving into much greater depth for each of the Big Three.

deploys a security-oriented set of domestic laws, institutions, and processes to establish the regulatory standards for intra-country and cross-border data flows. At the international level, it moves to exempt its domestic data regulations (including online content control and data localization measures) from international adjudications altogether, while safeguarding its cyber and data sovereignty against external pressures brought by the international trade or privacy regime.

Regarding the third research question, Chapters 2, 4, and 6 canvass the core mechanisms and factors enabling the diffusion of three dominant regulatory approaches at the international level, analyzing how the Big Three are shaping third countries' rulemaking for data governance.

Among them, Chapter 2 discusses two scenarios where U.S.-designed digital trade rules are diffusing among third countries. First, through strategic negotiations of high-standard international trade agreements to further trade liberalization (vertical forum-shifting), the U.S. was able to reach PTAs with trading partners on its desired terms, making these foreign governments sign up to U.S.-promoted data transfer provisions. Since PTAs are reciprocal in nature, the spread of the U.S. template of TPDF rules to other treaty parties is a natural and autonomous outcome of U.S.-led trade lawmaking processes.[114] Second, even when the U.S. is off the negotiation table, many third countries have incorporated U.S. digital trade rules on TPDF in their own PTAs, reflecting a growing international consensus that this template represents the most "advanced" model for developing the digital economy.

Chapter 4 deals with the increasing diffusion of EU data protection norms as the *de facto* international standards. It argues that this notable norm diffusion phenomenon is due to the Brussels Effect (both *de facto* and *de jure*), EU negotiators' skillful use of market power to pressure and incentivize third countries' to converge to EU data protection standards, the EU's deployment of issue-linkage, as well as the accessibility and normative appeal of EU norms for late-comer regulators.

Chapter 6 analyzes the mechanisms of influence that animate the diffusion of the Chinese data governance approach among a growing number of developing countries. These mechanisms include the Chinese government's vigorous norm promotion efforts (advocating for its vision of cyber and data governance internationally), Chinese firms' increasing supply of digital infrastructures to emerging markets (the Beijing Effect), and the normative appeal of the Chinese approach to like-minded Global South countries sharing more similarities to China than the West.

Finally, Chapter 7 summarizes the thesis's core arguments and major findings, and draws conclusive remarks on how the current regime complex that governs TPDF may influence domestic and international data regulations, generating normative and policy implications for transnational data governance.

[114] In that regard, this policy diffusion scenario is different from the cases of the EU and China, whose lawmaking and policy diffusion processes are separate and distinct. Given this reason and the word limit for the thesis, my discussion of the U.S.'s norm diffusion is much shorter than that of the EU or China (each of the latter has a standalone chapter).

Chapter 1

A Battle of the Big Three?
Competing Conceptualizations of Personal Data
Shaping Transnational Data Flows

Table of Contents

I. INTRODUCTION 31

II. THREE CONCEPTUALIZATIONS OF PERSONAL DATA WITH RESPECT TO TPDF 32

A. Personal Data as A Factor of Production 33

B. Personal Data as An Embodiment of Fundamental Rights 36

C. Personal Data as an Element of National Security 39

III. THREE COMPETING PARADIGMS UNDERGIRDED BY DIVERGENT CONCEPTUALIZATIONS 44

A. A Trade Paradigm to Regulate TPDF 44

(A) The Underlying Economic Logic 44

(B) Mega-Regional Trade Agreements 46

1. Free-Data-Flows Provisions 46

2. Provisions Against "Computer Localization" 48

3. Subjecting Measures Restricting TPDF to Investor-State Treaty Arbitration 48

4. Setting a Permissive Floor on Consumer Protection to Facilitate TPDF 49

B. A Fundamental Rights Paradigm to Regulate TPDF 53

(A) The Underlying Fundamental Rights Logic 53

(B) Protection of Privacy and Personal Data as Fundamental Rights 55

(C) A "Prohibition Subject to Limited Exceptions" Approach to TPDF 59

C. A National Security Paradigm to Regulate TPDF 64

(A) The Underlying National Security Logic 65

(B) An Institutional Framework Oriented at Safeguarding National Security 67

1. National Security Law 2015 67

2. Cybersecurity Law 2016 69

3. Personal Information Protection Law 2021 71

4. Data Security Law 2021 72

(C) The Cyberspace Administration of China as a Centralized Regulatory Authority 74

(D) Data Localization Subject to Limited Exceptions 75

IV. ADAPTING CONCEPTUALIZATIONS AND PARADIGMS 78

A. THE U.S. 78

B. THE EU 80

C. CHINA 83

V. CONCLUSION 86

I. Introduction

Despite surging scholarship on different approaches to regulating transborder personal data flows ("TPDF"), the underlying conceptualizations of personal data remain relatively undertheorized. However, the contestations on TPDF regulation often toggle among different conceptual framings of personal data, generating profound implications for our understanding of what personal data is and how TPDF should be regulated. To fill this gap, this chapter addresses divergent conceptualizations of personal data by three great powers, and provides a conceptual framework to explain their competing approaches to TPDF.[115]

Due to its hybrid nature, personal data is subject to three primary conceptualizations, ranging from economics to privacy to national security. With respect to TPDF regulation, the Big Three subscribe to different conceptualizations of personal data at a micro level, as well as divergent framings of the TPDF system at a macro level. In this regard, three different regulatory approaches has gained increasing prominence thus far:

1. *The dominant U.S. approach* to TPDF conceptualizes personal data as a factor of production, capable of fueling international trade, the data-driven economy, and transformative technologies. Focused on the economic interests of data, this conceptualization undergirds a trade-based approach to regulating TPDF, requiring free data flows across borders by default unless otherwise justified.
2. From a civil liberties perspective, *the prevailing EU approach* treats personal data as an embodiment of fundamental rights. Centered on the privacy value of personal data, this conceptualization justifies the EU-led fundamental rights-based approach, which requires high-standard protection of individuals' data privacy as the core criterion for allowing TPDF.
3. *The primary Chinese approach* to TPDF considers personal data as an element of national security. Based on this conceptualization, China deploys a security-oriented set of domestic laws, institutions, and processes to localize data storage within its borders—subject to limited exceptions (such as the government's security assessments) on relatively burdensome terms.

Albeit with their own nuances, these three primary conceptualizations cohere in key aspects. Highlighting different attributes of data, these conceptual framings diverge in their understanding of what personal data is, how a TPDF system should be designed, and on what terms personal data should be transferred across borders. Treating personal data as primarily a distinct object, each conceptualization differs in how they approach the relationship between individuals and their data, and in what they identify as the dominant interests at stake, as well as the most important normative goals for regulatory interventions.

[115] To be clear, the aim of this chapter is not to evaluate the substantive merits or practical feasibility of the proposals advanced by the Big Three. Rather, it seeks to provide an analytical framework to understand these superpowers' competing approaches to regulating TPDF, explaining the increasingly polarized debates on the regulation of this issue-area.

Moreover, these conceptualizations do not exist in vacuum, but rather are embedded in different philosophies and ideologies—ranging from neo-liberalism to human rights and to sovereignty—thereby entrenching their normative justifications and magnifying their ideational appeal. These irreducible normative elements render the contestations among these conceptualizations unable to be easily resolved, whether by empirical analysis or otherwise. At a deeper level, it is also infeasible to expect that the divergent interests underlying distinct conceptualizations could be easily bridged or reconciled by the Big Three. In the medium term, these three primary conceptual framings and regulatory approaches may co-exist, compete, and interact with each other in great powers' geo-political and economic competition.

This chapter further explores the implications of these conceptualizations for the (re)design of the emerging legal and regulatory framework to govern TPDF. Different *conceptualizations* of personal data warrant and justify distinct legal *paradigms*. Aligned with their primary conceptualizations, the Big Three deploy divergent paradigms to institutionalize their fundamental choices, and to provide legal prescriptions and enforcement tools to address the salient problems framed in different ways. Notably, these competing paradigms diverge from each other in their own basic logic, normative justifications, and legal solutions. Regulation of TPDF is increasingly caught among these competing conceptualizations and paradigms, which race to claim authority to govern the decision-making process. By and large, why the proper balance among three distinct interests (or values) of personal data (i.e., economics, privacy, and national security) remains so contestable is because the desired equilibrium looks starkly different, depending on which conceptualization is engaged and which paradigm the policymaker is situated in.

The remainder of this chapter is structured as followed. Section II unpacks the Big Three's dominant conceptualizations of personal data with respect to TPDF regulation. Focused on the conceptual underpinnings, it parses the normative content of these conceptualizations, as well as the discourses and ideologies which they are embedded in. In Section III, this chapter delves into the Big Three's primary legal paradigms to regulating TPDF, discussing the implications of different conceptualizations for the regulatory design to govern this issue-area. Undergirded by distinct conceptualizations, three dominant paradigms provide divergent substantive rules and enforcement tools to serve the Big Three's prioritized policy goals. Section IV briefly reviews how three great powers adapt their conceptualizations and paradigms to accommodate each other and to balance their shifting interests. Section V draws conclusive remarks.

II. THREE CONCEPTUALIZATIONS OF PERSONAL DATA WITH RESPECT TO TPDF

In the digital era, personal data is a hybrid, *sui generis* element, primarily consisting of components of economics, privacy, and national security. Economically, big data on scale becomes the new "oil" of the global digital economy, fueling the development of digital services, e-commerce, data-driven business models, and cutting-edge technologies (such as Artificial Intelligence ("AI")). Meanwhile, personal data carries digitalized information about a data subject, embodying individuals' privacy interests crucial to the achievement of human dignity, civil liberties, and self-determination. Finally, access to and control of sensitive personal data could expose the vulnerabilities of national security to a threat actor (whether private or public), implicating mass surveillance, digital espionage, cyber warfare, as well as a state's sovereignty exercised in cyberspace.

In essence, conceptualization of personal data is a value-laden social construction. With respect to cross-border data flows for commercial purposes, personal data could be primarily conceptualized as (i) a factor of production driving the digitalized economy, (ii) an embodiment of individuals' fundamental rights essential to dignity, autonomy, and personality; and (iii) a building block undergirding national security. The U.S., the EU, and China subscribe to each of them, respectively, as their primary (yet not mutually exclusive) conceptualizations of personal data with respect to TPDF regulation. Importantly, divergent conceptualizations reflect different normative objectives, policy priorities, and trade-offs, while serving distinct interests and values. How personal data is conceptualized could highlight or downplay its different attributes, influencing how a policy problem is defined and what legal solutions are designed in response.

A. Personal Data as A Factor of Production

The dominant U.S. conceptualization views personal data as a digital factor of production (resource, raw material, or asset) that can drive the development of international trade, the data-driven economy, and transformative technologies.[116] Generated through cyberspace transactions and people's interactions with the digital interface, personal data is captured as an intangible "asset" by digital firms for commercialization. Comparable to traditional factors of production (such as capital, labor, land), personal data becomes an intangible input crucial for modern economic production and business operation.[117] The discussion below analyzes the key assumptions and normative content of this conceptualization.

First, though originating from individuals (as service users or customers), personal data may become an intangible "asset" of digital firms through a transaction (whether free or not). By signing up to the terms of a service agreement, data subjects frequently transfer the right to access, control, use, and exchange their data to digital firms, as sort of a "consideration", in exchange for the provision of digital services or products.[118] In nature, this process is a contractual "transaction", characterized by a transfer of value based on mutual consent. As a result, digital firms would

---

[116] See e.g., Office of the United States Trade Representative, Trans-Pacific Partnership Agreement, art. 14.8(1)-(2), https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf; the United States-Mexico-Canada Agreement ("USMCA"), effective on July 1, 2020, art. 19.8 ("1. The Parties recognize the *economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade*. 2. *To this end*, each Party shall adopt or maintain *a legal framework that provides for the protection of the personal information* of the users of digital trade.") (emphasis added). See also Sveltlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV., 416, 499 (2020) (arguing that the U.S.'s digital trade discourse "tends to equate strict privacy and data protection measures such as restrictions on cross-border data flows with a non-tariff trade barrier and, potentially, digital protectionism. However, even when some degree of privacy and data protection *are* factored into this discourse of digital trade, the protection of these interests is often presented as an *economic* necessity, a precondition for free trade rather than a fundamental right and societal value beyond its economic utility. It is likely presented as such because the use of the digital protectionism label features trade values as natural and obvious and forces policy makers to defend the measure against a baseline of free trade as non-protectionist. Regulatory conversations on privacy and data protection within the economic digital trade discourse about the term 'digital protectionism' thus implicitly bring in the normative goal of maximization of wealth….").

[117] Milton Muller & Karl Grindal, *Data Flows and the Digital Economy: Information as A Mobile Factor of Production*, 21 DIGITAL POLICY, REGULATION AND GOVERNANCE, 71, 72 (2019).

[118] Chris Hoofnagle, *Facebook and Google Are the New Data-Broker*, CORNELL TECH, https://hoofnagle.berkeley.edu/wp-content/uploads/2018/12/hoofnagle_facebook_google_data_brokers.pdf.

acquire a property-like right to control personal data as a digital asset, which can be utilized to serve their commercial interests.

To be clear, by "digital asset", I do not mean that personal data per se has been incorporated into these companies' balance sheets. Rather, by collecting and controlling an enormous amount of personal data, digital firms could monetarize the economic value of such data. This could occur in numerous ways, including the provision of data as a service (such as various transactions involving the rights to access and use personal data),[119] the provision of insights derived from data as a service (e.g., predicative analytics for targeted advertisements), as well as the provision of an analytics-enabled digital platform as a service.[120] Further, digital firms could also leverage the control over their data base and digital ecosystems to entrench their market power.[121] Indeed, nowadays the dominant market power of a handful "Big Tech" firms increasingly stems from their collection, use, and exploitation of personal data.[122] Either way, digital firms today are capable of transforming data from a raw material (or resource) into a capitalized property, which becomes increasingly important for the existence, expansion, and dominance of their business models.[123]

Second, traded like a commodity in the market, personal data becomes something that the data subject should contract for with digital firms when negotiating a transaction in cyberspace.[124] This makes the protection of personal data primarily a matter of consumer protection to be balanced with efficient business transactions, as opposed to a fundamental right trumping other interests. Indeed, consumer protection also helps to constrain and balance digital firms' rights to collect, control, transfer, and commercialize personal data at will. However, under this conceptualization, data privacy protection becomes more of "a precondition for digital trade",[125] as well as a qualification to digital capitalism's property rights to data.

Third, through this economic lens, the most prevalent interest underlying TPDF is data's economic value, and the issue of TPDF becomes primarily a matter of economics. To be clear, unprocessed

---

[119] Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construction for Moving Forward*, 16 DUKE LAW & TECHNOLOGY REVIEW 220, 222-23 (2018) (noting that with the construction of a property right to data, "both existing and new types of transactions can be more formally expressed (e.g., licenses, sales, transfers, processing services, storage services, analytics, and more)… Sales transactions, licensing deals, joint ventures, downstream distributions and syndications of rights to access and use data, valuation for accounting and tax purposes—all of these are possible, and some are already occurring.").

[120] Major ways to monetize data include provision of data as a service (including various transactions involving rights to access and use personal data), provision of insights derived from data as a service (such as predicative analytics for targeted advertisements), and provision of analytics-enabled platform as a service. See Krzysztof Goworek, *Data Monetization—How to Monetize Data Successfully*, TASIL INSIGHTS (August 30, 2019), https://tasil.com/insights/data-monetization-business-strategy/.

[121] Kean Birch et al., *Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech*, BIG DATA & SOCIETY 1, 2, 13 (2021).

[122] *Id*., 1-2. Tom Wheeler, ex-Chairman of US Federal Communications Commission (2013–2017), put it this way: "It was the 'Wizard of Oz' in digital format as the four titans of Big Tech testified via video before the House Antitrust Subcommittee. Just like in the movie, what the subcommittee saw was controlled by a force hidden from view. The wizard in this case – *the reason these four companies are so powerful – is the math that takes our private information and turns it into their corporate asset*." (emphasis added)

[123] Birch et al., *supra*, 2, 13.

[124] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STANFORD LAW REVIEW 1193, 1193 (1998). Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 121 (2017).

[125] Yakovleva, *supra* note, 492.

individual data is usually economically "worthless". Rather, the economic value of big data could be materialized only when data collected at scale has been processed by big data analytics algorithms and complex computational applications.[126] In this process, digital firms are often credited with "spinning straw into gold" for their indispensable role in realizing data's monetary value.

Economically, the more data that flows across countries, the lesser the transaction costs for digital firms to access and leverage data, and the greater the likelihood that data could develop the digital economy and transformative technologies to the utmost extent. Following this logic, the primary policy goals of the law to govern TPDF should be to maximize the economic value of data, to reduce transaction costs, to boost efficiency and economies of scale, to enhance the prosperity of the data-driven economy, and to spur technological advancement.[127] In contrast, other values underlying personal data—including privacy and national security—become exceptional grounds for occasional departure from the default rule of "free data flows".

It follows that with respect to regulating personal data, the market should serve as the predominant mechanism to price data correctly and allocate it efficiently.[128] Guided by the principle of efficiency, this conceptualization requires a marketplace approach to regulating TPDF, relying primarily on digital firms' self-regulation to deal with the potential negative externalities.

Moreover, this economic conceptualization of personal data is embedded into a broader normative framework of neoliberalism (the "Washington Consensus") and a "market fundamentalist" ideology. Under a neoliberal view, governmental intervention into the market should be reduced to a minimum, and any regulation may amount to a potential trade barrier.[129] This approach largely relies on the theory of "regulatory capture": any regulation is almost inevitably subject to capture by organized interest groups, which would eventually reduce social welfare, rather than serving public interests.[130]

This neoliberal approach to domestic regulation was sharpened by what Joseph Stiglitz termed a "market fundamentalist" ideology, advocating that "free, unregulated markets were the best way to organize a society."[131] Under the assumption that public policy goals generally can be more

---

[126] Chun-Wei Tsai et al, *Big Data Analytics: A Survey*, 21 JOURNAL OF BIG DATA 1, 16-20 (2015) (introducing data mining algorithms and machine learning); See Big Data Analytics—What It Is and Why It Matters, https://www.sas.com/en_hk/insights/analytics/big-data-analytics.html (noting that big data analytics is an important process to examine huge sum of data to extract meaningful insights, including hidden patterns, market trends, correlations, customer preferences, and other insights, and it could be used to improve decision-making, strengthen targeted marketing, identify and prevent fraud, achieve effective business management).

[127] Shaffer, *supra* note, 262.

[128] Kang, *supra* note, 1201.

[129] See eg. CASS SUNSTEIN, AFTER THE RIGHTS REVOLUTION 70 (1993).

[130] Dongsheng Zang, *Divided by Common Language: "Capture" Theories in GATT/WTO and the Communicative Impasse*, 32 HASTINGS INT'L & COMPARATIVE L. REV. 423, 425 (2009) (noting that the "'capture' theory actually set the theoretical foundation of the institutional design of the WTO."). See also JAN TUMLIR, PROTECTIONISM 4 (1985); JOHANNES OVERBEEK, FREE TRADE VERSUS PROTECTIONISM 558 (1999).

[131] Yakovleva, *supra note*, 453-454. See JOSEPH E. STIGLITZ, GLOBALIZATION AND ITS DISCONTENTS REVISITED xl (2018) ("Doubling down on the Washington Consensus was a policy inspired by the special interests that it served, but the belief in the efficacy of these policies was supported by 'market fundamentalist' ideologies—the notion that free, unregulated markets were the best way to organize a society.").

efficiently achieved by domestic regulation not interfering with international trade, this ideology argues that unfettered international trade creates optimal efficiency gains and maximizes domestic welfare, meanwhile downplaying the associated negatives (such as domestic distributional effects that create winners and losers).[132]

Against such a normative background, this economic conceptualization of personal data lends support to transposing the policy rationale for "free trade flows" to justify "free data flows", thereby squarely situating the regulation of TPDF under the rubric of international trade law. By treating data flows as a natural, logical, and automatic extension of trade liberalization agenda, this conceptual framing implicitly adopts neoliberal prescriptions as the default rules, drawing on various assumptions and inferences consistent with that school of thought.

Since free trade flows work best in maximizing global economic welfare ("rising water lifting all boats"), so too should transnational personal data flows be unrestricted. As such, domestic regulations at odds with the benchmark of economic efficiency may constitute non-tariff "barriers" to digital trade, and thus are placed "in an a priori defensive position."[133] Consequently, any regulatory actions inconsistent with the "liberalization" agenda and "free data flows" prescription become a deviating exception, and are required to be somehow justified, lest a breach of international trade rules may arise. And governmental regulation should focus on ensuring unrestricted data flows and correcting acts of digital "protectionism", which is defined as governments' unjustified deviations from the baseline position of optimal market efficiency.[134]

B. Personal Data as An Embodiment of Fundamental Rights

The prevalent European conceptualization treats personal data as an embodiment of fundamental rights of individuals.[135] With the increasing ubiquity of cyberspace where people carry out a myriad of transactions and daily activities, modern communication technologies often enable continuous, cumulative, and invisible observations of our lives, potentially creating wide-spread and pervasive online surveillance.[136] Though much personal data is anonymized when processed in large troves, the rapid advancement of "reidentification" technologies could increasingly

---

[132] Yakovleva, *supra* note, 453.
[133] *Id*., 427.
[134] *Id*., 430 (noting that in international trade law, the "core issue in defining protectionism is where to draw the line between regulation that is a precondition for trade (such as state intervention aimed at correcting market failures, which is economically efficient and socially more productive), and protectionist regulation which creates market failures and stifles trade.").
[135] See e.g., Charter of Fundamental Rights of the European Union, 2000 O.J. C 364/10, art. 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) ["EU Charter of Fundamental Rights"]; EUROPEAN DATA PROTECTION SUPERVISOR, OPINION 4/2015, TOWARDS A NEW DIGITAL ETHICS: DATA, DIGNITY AND TECHNOLOGY, September 2015, at 4 ("The fundamental rights to privacy and to the protection of personal data have become more important for the protection of human dignity than ever before. They are enshrined in the EU Treaties and in the EU Charter of Fundamental Rights. They enable individuals to develop their own personalities, to lead independent lives, to innovate and to exercise other rights and freedoms. The data protection principles defined in the EU Charter…."), https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf ["OPINION 4/2015"].
[136] Kang, *supra* note, 1193.

"deanonymize" or "reidentify" anonymized data with relative ease.[137] In particular, large volumes of personal data could be hacked, misused, and manipulated, endangering individuals' privacy, human rights, and civil liberties. Overall, this conceptualization focuses on the significant risks imposed by personal data processing to these essential interests at stake.

First, this conceptualization centers on individuals whose personal data is processed, privileging them as bearers of fundamental rights.[138] In this light, the treatment of individuals' personal data becomes an issue of fundamental rights protection, anchored in the primary interests of human dignity, personal integrity, and self-determination.[139] This rights-based framing stands in stark contrast with the economic conceptualization, since the latter perceives individuals as consumers whose data is traded in the market like a commodity, and thus situates data subjects "squarely in the marketplace relations."[140]

Second, from this conceptual framing, personal data represents an embodiment of fundamental rights in the first place, implicating important interests of human rights and civil liberties. In comparison, the economic value of data is of a secondary and derivative nature, and represents a byproduct generated by data processing.[141] The same goes for national security interests. Under this logic, the privacy value of personal data should be elevated to a primary position, compared to associated economic implications and other interests involved. And in case of conflicts, the normative weight of fundamental rights underlying personal data could override other interests implicated by data flows. As a result, with respect to data transfers (as a form of "processing"), individuals' data privacy should be adequately protected as a normative priority, even at the cost of sacrificing certain economic utility. Such a normative priority thus sharply contrasts with the economic conceptualization, which focuses on maximizing personal data's commercial potential as a primary concern.

---

[137] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA LAW REVIEW 1701, 1703-1704 (2010) (arguing that contrary to conventional wisdom, data anonymization does not ensure adequate privacy: "[d]ata can be either useful or perfectly anonymous but never both."). Kelsey Campbell-Dollaghan, *Sorry, Your Data Can Still be Identified Even If It's Anonymized*, FASTCOMPANY (October 12, 2018), https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized (a group of MIT scientists and urban planners found that even anonymized data could be deanonymized quickly when crossing multiple data sets and applying algorithms).

[138] See e.g., EU Charter of Fundamental Rights, art. 7, 8(1); EUROPEAN DATA PROTECTION SUPERVISOR, *supra* (OPINION 4/2015), 4.

[139] Schwartz & Peifer, *supra* note, 123, 126-127. See eg. Act 1978-17 of 6 January 1978, Data Protection Law, art. 1 (Fr.), *translation at* https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf [https://perma.cc/4759-7WVT] (article 1 of the 1978 French national data protection law proclaimed that information technology "shall not violate human identity, human rights, privacy, or individual or public liberties.") See also BVerfG, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil) (Census case), Dec. 15, 1983 (the German Federal Constitutional Court in the *Census* case famously stated that personal data processing endangers individuals' decisional authority as well as the existence of "a free democratic community based on its citizens' capacity to act and participate.").

[140] Schwartz & Peifer, *surpa* note, 132.

[141] See Yakoleva, *supra* note, 506 ("Although the European Union embraces both economic and moral value approaches to the protection of privacy and personal data, the latter will always prevail because the European Union may neither conclude nor implement through an E.U. legislative act an international agreement or decision of an international adjudicating body if it does not comply with the E.U. Charter."); see also Milton Mueller & Karl Grindal, *Is It "Trade?" Data Flows and the Digital Economy*, at 10, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137819.

Under this fundamental rights framing, the primary problem plaguing TPDF regulation becomes a human rights and civil liberties issue: namely, how to safeguard individuals' data privacy against potential intrusions by foreign private and public actors, given that the processing of personal data imposes an inherent threat to data subjects' fundamental interests of human dignity, personality, and individual autonomy. To be clear, it is not that the economic value of data is unimportant. Rather, it is only after the fundamental rights are adequately protected that personal data should become capable of being monetized or commodified. In parallel, national security interests are important, but a state typically could protect its national security interests underlying personal data by enforcing a robust and comprehensive data protection framework.[142] Given the fundamental rights status of data privacy protection, TPDF regulation should prioritize high-standard data protection as an overarching purpose of the regulatory design.

Third, following this logic, personal data is too important to be traded or contracted away by individuals in the marketplace. Just like other fundamental rights, the legal entitlements to personal data belong to the data subjects, and are only partially alienable. Also, given the unequal bargaining power between an individual and a digital firm (especially those "Big Tech" giants), a data subject's consent to transfer the right to control and use their data may not be taken for granted—at least might not be worth its face value. Thus, under this framing, the relationship between individuals and their personal data is substantially different from that of the economic conceptualization, which holds that people in the marketplace engage in free exchanges concerning their personal data largely out of self-interest.[143]

Further, digital firms, having unparalleled access to and control of personal data, should be bound to act as a form of "trustee" responsible for maintaining high-standard data protection, otherwise a breach or improper use of data may result in significant legal liabilities. This *trustee-like* obligation to diligently safeguard the interests of data subjects transcends the *customer-vendor* relationship between individuals and digital firms under the economic framing of personal data.

Under this rights-based conceptualization, relying primarily on the market mechanisms to protect data privacy is far from satisfactory, since this self-regulation approach creates conflicts-of-interest problems at an institutional level (*i.e.*, the dual role of digital firms as self-regulators and data-reliant businesses simultaneously),[144] potentially resulting in a race-to-the-bottom. To prevent market malfunctioning, the regulatory state thus should step in to implement and enforce a pervasive regulatory system to adequately protect individuals' data privacy. Meanwhile, data subjects should be vested with robust legal rights to hold digital firms accountable for breaches of

---

[142] See Susan Ariel Aaronson, *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*, CIGI PAPER NO. 241 (April 15, 2020), at 19 https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves/.

[143] Schwartz & Peifer, *supra* note, 132.

[144] Aaronson, *supra* note, at 6 (noting "Big Tech" giant firms generally "have many incentives to utilize and monetize data and fewer incentives to protect data, despite its effects on trust."). To be clear, it is not that private-sector actors are inherently untrustworthy or morally corrupted. Rather, their prime motivations to seek commercial profits would create "conflicts of interest" scenarios, which may undermine their efforts to effectively police data privacy. In other words, the basic logic of economic efficiency of an economic conceptualization proves starkly unfit with the normative priority of fundamental rights protection.

their data privacy before specialized regulatory authorities or courts entrusted with protecting fundamental rights and civil liberties.

At a deeper level, this rights-based conceptualization is part of a broader fundamental rights culture, which has experienced substantial growth in Europe in recent decades.[145] In the grand project of forging deeper political cooperation and integration through pan-European political institutions, one of the major hurdles is the "democratic deficit" of these supranational organizations in the eyes of European citizens.[146] A viable response to address this problem is to develop and enforce a common set of "European constitutional rights", including—most notably—fundamental rights.[147]

In this context, the EU-level institutions are expected to provide European citizens with common "constitutional guarantees of justice and freedom", with human dignity being the bedrock thereof.[148] European data protection law has been at the forefront of such efforts, and now becomes an important part of European human rights law.[149] Notably, the rights-based conceptualization undergirds the common European language of data protection law. In this way, such a conceptual framing of personal data has been incorporated into a broader project—the development of a pan-European political identity based on shared fundamental rights.

C. Personal Data as an Element of National Security

The primary Chinese conceptualization views personal data as an indispensable element of national security.[150] By "national security", I refer to the requirements for the government to protect the state and its citizens against various security threats and national crises, in order to maintain the safety, legitimacy, and wellbeing of the state.[151] Since it is ultimately composed of individuals, a sovereign state may become vulnerable when the data of its people is breached and exploited by a rival state or hostile forces. In particular, digital firms and governmental agencies that collect and process large troves of personal data could be targeted by foreign intelligence

---

[145] Schwartz & Peifer, *supra* note, 126, 145.

[146] PAUL CRAIG & GRÁINNE DE BÚRCA, EU LAW: TEXTS, CASES, AND MATERIALS 58 (2008).

[147] Schwartz and Peifer, *supra* note, 145.

[148] *Id.*

[149] *Id.*, 146.

[150] See e.g., National People's Congress, *Cybersecurity Law of the People's Republic of China*, promulgated in November 2016, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml, art. 1 ("the enactment of this law is for the purposes of protecting cybersecurity, safeguarding cyber sovereignty and national security….") ["Cybersecurity Law 2016"]; National People's Congress, *Data Security Law of the People's Republic of China*, promulgated in June 2021, art. 1 ("the enactment of this law is for the purposes of regulating data processing activities, safeguarding data security, promoting the use and exploitation of data, protecting the legitimate rights and interests of individuals and organizations, and safeguarding *national sovereignty*, *national security*, and development interests") (emphasis added), http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml ["Data Security Law 2021"].

[151] Aaronson, *supra* note, 2 ("National security refers to the requirement to maintain the legitimacy and survival of the state. In a viable and healthy nation, citizens trust their government, live in a stable and growing environment, and generally feel safe and secure. Security threats can include warfare, terrorism, economic conflict, digital attacks, malicious non-state actors…"). Julien Chaisse, *Demystifying Public Security Exception and Limitations on Capital Movement*, 37 U. PENN. J. INT'L L. 583, 596 (2015) (noting that "national security" requires a government to "protect the state and its citizens against all kinds of 'national crises'.")

authorities, terrorists, or criminals, creating genuine threats to national security. While identifying a security risk does not equate with the realization of that threat, from a national security perspective, a threat actor's capability of causing or exploiting harm often translates into a state's strategic vulnerability, particularly if the underlying national interests are important enough. It follows that the security and control of personal data may become a matter of national security, and thus could top a state's priority list, irrespective of the potential costs to economic efficiency and other values concerned.

First, large amounts of personal data could be stolen, hacked, misused, and exploited in ways that pose imminent risks to a state's national security. Threat actors may use hacked sensitive personal data to blackmail, extort, and intimidate the data subjects—especially politicians, officials, governmental personnel, and public figures—thus facilitating crimes, espionages, and political infiltrations.[152] By exploiting a digital vulnerability (such as the lack of a robust data privacy protection system), an enemy or criminals may use personal data to identify, stalk, and target military members and their families as a novel act of war or terror.[153] When cross-referenced with other data sets, large troves of aggregated anonymized personal data could identify sensitive groups of individuals (such as military officers or high-profile politicians), and reveal a government's classified strategies and objectives, as well as military and defence information.[154]

Second, with respect to key information and telecommunication infrastructures, relying on foreign firms that are affiliated to a rival state or subject to the latter's jurisdiction risks creating "weaponized interdependence."[155] If a foreign government could coerce, compel, or legally require a private firm to hand over vast amounts of personal data it collected from a host state, the underlying digital infrastructure may be turned into a surveillance machine and a vehicle for espionage, generating "panopticon effects" and endangering national security interests.[156] In particular, since the use of data is nonrival and only partially excludable and that data may never vanish once obtained, digital firms cannot effectively guarantee in advance that they would not share personal data with a government, creating huge uncertainties over the potential future use of data.[157] This commitment problem looks more problematic for digital firms based in an authoritarian country, due to the oftentimes blurring boundary between the public and private sectors there, as well as the lack of robust institutional rule-of-law constraints to check the abuse of public power.[158]

Also, such a threat to national security may be pressing for digital firms from a liberal democracy with a track record of government-led mass surveillance operations (such as U.S. National Security

---

[152] See Josie Le Blond, *German Politicians' Personal Data Leaked Online*, THE GUARDIAN (January 4, 2019), https://www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online.
[153] Sarah Albrycht, *When the Homefront Becomes the (Cyber) Front Line*, FIFTH DOMAIN (February 3, 2020), https://www.fifthdomain.com/opinion/2020/02/03/when-the-homefront-becomes-the-cyber-front-line/.
[154] Aaronson, *supra* note, 3.
[155] Henry Farrell & Abraham Newman, *Weaponized Globalization: Huawei and the Emerging Battler over 5G Networks*, 14 GLOBAL ASIA 8, 9-10 (2019).
[156] *Id.*, 10. See Sinéad Baker, *The New York Times Was Able to Track Trump's Movements with Leaked Location Data, Showing How Easy It Is to Spy on People Via Their Phones*, INSIDER (December 20, 2019), https://www.businessinsider.com/nyt-tracked-trump-leaked-location-data-mobile-phone-spying-easy-2019-12
[157] Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUDIES IN COMPARATIVE INTERNATIONAL DEVELOPMENT 45, 47 (2021).
[158] *Id.*, 57, 60.

Agency's PRISM project). This explains why in the aftermath of the Edward Snowden revelations, the Chinese government has repeatedly underscored the importance of ensuring cybersecurity and protecting against U.S. intelligence surveillance, cyber espionage, digital infiltrations, and other cyber interferences, as reflected in President Xi's dictum that "there can be no national security without network security".[159]

Third, foreign intelligence operations could exploit massive troves of personal data to systemically spread online misinformation and manipulate public opinion. Throughout history, adversaries have used disinformation to create divisions and undercut "trust and societal cohesiveness".[160] Yet, with the advancements in technology to collect and process big data, this risk becomes increasingly problematic today. For a democratic society, an organized foreign misinformation campaign that exploits vulnerabilities in its data governance system may substantially interfere with important domestic political processes. A case in point is Cambridge Analytica, suggesting that seemingly innocuous personal data sets harvested from a popular social media platform could be leveraged by foreign intelligence agencies to manipulate elections, including of presidential candidates.[161]

As for authoritarian regimes, the materialization of this risk could undermine the legitimacy of the ruling regime, making a country's political and social stability vulnerable to attack by an adversarial state. For China, the most relevant case to illustrate this risk is the "Arab Spring", which effectively brought down the incumbent political regimes in some Arab countries in the early 2010s.[162] Given the pervasive influence of social media platforms over a society's population at large, it conceivable that a mass of personal data could be exploited and weaponized by an adversary's intelligence operations to manipulate and influence the general public's perceptions on the legitimacy of a political regime (or a model of governance), undercutting important ideological interests.[163] In this way, data security could threaten a country's "political security" and "social stability", which China have long framed as a core tenet of its national security, especially after the collapse of the Soviet Union.[164]

While these three risks identified are mostly concerned with "data security", the fourth threat relates to a broad notion of "economic security". Given that data has become a strategic resource

---

[159] John Chen et al., *China's Internet of Things*, RESEARCH REPORT PREPARED ON BEHALF OF THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (October 2018), at 8, https://www.uscc.gov/sites/default/files/Research/SOSi_China%27s%20Internet%20of%20Things.pdf.

[160] Aaronson, *supra* note, 4.

[161] Chen, *supra* note 6.

[162] See Nahed Eltantawy & Julie B. Wiest, *Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory*, 5 INT'L J. COMMUNICATIONS 1207 (2011).

[163] See Anupam Chander & Haochen Sun, *Sovereignty 2.0*, GEORGETOWN LAW FACULTY PUBLICATIONS AND OTHER WORKS. 2404, UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPER NO. 2021/041 (2021), at 12 (arguing that "(w)estern 'information freedom' approach to the internet is perceived as a threat to 'Chinese ideological security'" and that "the Chinese government instead seeks to use the internet to consolidate party control, maintain social order and proliferate desirable socialist and Confucian values such as 'patriotism,' 'loyalty to the communist party,' 'dedication to one's work,' 'honesty,' [and] 'filial piety,' to 'develop a cohesive, socialist nation.').

[164] Marc Julienne, *Xi Jinping's Conquest of China's National Security Apparatus*, FRENCH INSTITUTE OF INTERNATIONAL RELATIONS (July 1, 2021), https://www.ifri.org/en/publications/publications-ifri/xi-jinpings-conquest-chinas-national-security-apparatus; CPC Central Committee Bimonthly QiuShi, *Safeguard National Security and Social Stability*, originally in XI JINPING, THE GOVERNANCE OF CHINA I, December 7, 2020, http://en.qstheory.cn/2020-12/07/c_607612.htm.

crucial for the digital economy and machine-learning algorithms, the control and use of big data could significantly influence a state's "economic security", which is an important part of its "national security".[165] Since it is economic power that eventually undergirds other forms of power—including military power, which is generally understood in zero-sum terms by great powers—a superpower's competitive edge in the data-driven economy and transformative technologies (such as AI) could turn into its military and strategic advantage over a geopolitical competitor.[166] Also, dependence on a rival state for the supply of critical dual-use technologies essential for economic development and military force (such as 5G and semiconductors) could result in vulnerabilities for national security, which can be weaponized by that state for economic, military, and political purposes.[167] Thus, in the global tech race and geopolitical rivalry, which great power can use big data to dominate the digital economy and AI-driven technologies may significantly influence regional and international balance of power, profoundly affecting a state's national security.

Under this conceptualization, security is not only a desired outcome, but represents the ultimate purpose of all nation-states.[168] As economically valuable as it could be, trade should always remain a secondary consideration, since only if security is ensured could a state safely pursue other goals, whether monetary or not.[169] Likewise, individuals' privacy may be important, but the provision of such a public good is subject to a more fundamental precondition: the security of the state. Otherwise, the existence of the institution to enforce human rights and to create the conditions for individuals to flourish may be threatened in the first place.

Under this logic, trade is "a peacetime privilege", a "lever of power", as well as "a wartime tool", rather than an unconditional "right" in itself.[170] This understanding of the relationship between security and trade is fundamentally different from the economic conceptualization, which focuses on economic welfare and efficiency as the normative priorities, and views national security as an exception to be otherwise justified. Similarly, under this security-oriented framing, individuals' data privacy is a secondary concern, compared with the fundamental issue of national security.

For policymakers who embrace the economic framing of personal data, this security-oriented conceptualization is problematic, as it risks creating "protectionism" in disguise. Indeed, sometimes, there may be an overlap between genuine national security concerns and protectionist considerations. And by treating economic security as national security, it might be increasingly difficult to draw a clear-cut boundary between measures that protect national security with

---

[165] For why economic security is national security, see generally Peter Navarro, *Why Economic Security Is National Security*, REALCLEAR POLITICS (December 9, 2018), https://www.realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security_138875.html; Edward Luttwak, *From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce*, 20 THE NATIONAL INTEREST 17 (1990).

[166] See Anthea Roberts et al., *Toward A Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECO. L 655, 659 (2020).

[167] *Id.*, 659-660. Newman & Farrell, *supra* note, 11-12.

[168] Harlan Grant Cohen, *Nations and Markets*, 23 J. INT'L ECO. L. 793 801-802 (2019) ("security is… shorthand for the Hobbesian view that society and state exist for fundamental purpose of providing security against the savagery of others. Security and state in this view are one and the same.")

[169] *Id*. KENNETH WALTZ, THEORY OF INTERNATIONAL POLITICS 126 (1979).

[170] Cohen, *supra* note, 800, 802.

protectionist measures, particularly under a less intrusive good-faith test.[171] However, under this security framing, the point is not how to precisely distinguish protection from protectionism. Rather, the real question is whether and how the national security concerns could be adequately addressed, regardless of the attendant economic costs. In other words, by focusing on national security as a primary concern, the security conceptualization requires a fundamental logic that is starkly different from the economic framing.

Finally, in the case of China, this security framing of personal data is anchored in an earlier notion of "cyber sovereignty" (also known as "information sovereignty").[172] In the early 2010s, China actively promoted the discourse of "cyber sovereignty" to push back against a U.S.-led campaign that advocated global Internet freedom as a universal "freedom to connect".[173] As emphasized by China's vision of "cyber sovereignty", traditional state sovereignty should be expanded to the "information frontier" (or the cyberspace), and managing online information flows is an important sovereignty right of a nation-state under public international law.[174] As articulated by China in its 2010 White Paper, "(w)ithin Chinese territory the Internet is under the jurisdiction of Chinese sovereignty", and thus China's cyber sovereignty over the Internet "should be respected and protected", such that its domestic Internet governance model and policymaking should be free from any foreign interference.[175] The link to territoriality is grounded on the traditional Westphalian notion of territorial-based sovereignty, while reflecting China's long-standing foreign policy pledging non-interference in foreign countries' internal affairs.[176]

By invoking "cyber sovereignty" to safeguard cybersecurity and national security, China seeks to legitimize its stringent governmental control of online content (i.e., Internet filtering and censoring) within its territory.[177] Consistent with this underlying logic, China's security-oriented

---

[171] Roberts et al., *supra* note, 665 (noting that this could "create a permanent state of exception justifying broad protection/protectionist measures across time and space").

[172] See Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 NYU J. INT'L L. POLITICS 36 (2021) (noting that "China has consistently articulated a vision for global Internet governance that emphasizes governmental control over data flows under the rubric of cyber sovereignty and, more recently, data sovereignty.")

[173] See MICHAEL JABLONSKI & SHAWN M. POWERS, REAL CYBER WAR 6-11 (2015) ("On January 21, 2010, Secretary of State Clinton delivered a seminal speech, 'Remarks on Internet Freedom,' at The Newseum in Washington, D.C… (which) deployed historically charged, ideological language alongside contemporary anecdotes emphasizing the endless, collective possibilities of ubiquitous internet connectivity."), 13-15.

[174] See People's Daily (Renmin Ribao), January 25, 2010, via *id*. 14; see id. 13-15. Erie & Streinz, *supra* note, 24 ("The notion of 'cyber sovereignty' (*wangluo zhuquan*), the idea to assert national jurisdiction over the Internet in China, is central to its data governance regime and shapes how Chinese citizens engage with the outside world and vice versa"), 36. For a detailed discussion on China's vision of "cyber sovereignty", see *supra* chapter 5 ("China's Data Sovereignty"), section I.B.

[175] Information Office of the Chinese State Council, *White Paper on the Internet in China*, CHINA DAILY (June 8, 2010), https://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm. See Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 399 (2020).

[176] Chander & Sun, *supra* note, at 11 (noting that according to President Xi Jinping, "respecting cyber-sovereignty" requires "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace — avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries.").

[177] For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section I.B. See also State Council, *White Paper* ("Internet security is a prerequisite for the sound development and effective utilization of the Internet … Effectively protecting Internet security is an important part of China's Internet administration, and an indispensable requirement for protecting state security and the public interest.").

conceptualization of personal data underpins a notion of "data sovereignty", which is a new central front of "cyber sovereignty" in the digitalized era. Notably, "data sovereignty" is the sovereign power of a state to exclusively govern domestic and cross-border data flows, based on its territorial jurisdiction over digital infrastructures located within its borders.[178] With respect to TPDF regulation, China treats cybersecurity and national security as central goals for the exercise of its data sovereignty. Otherwise, unconstrained data flows free from governmental intervention may render the country's control, filtering, and censorship of online information more cumbersome, less manageable, thereby jeopardizing domestic political stability and the party-state's ruling.[179]

III. THREE COMPETING PARADIGMS UNDERGIRDED BY DIVERGENT CONCEPTUALIZATIONS

With each emphasizing a particular attribute of personal data, three primary *conceptualizations* undergird and justify distinct *paradigms* as the primary field of law to govern TPDF, generating significant implications for the (re)design of the TPDF framework. In the global regulatory environment, the regulation of TPDF is increasingly caught between three dominant legal paradigms—namely, a trade paradigm, a fundamental rights paradigm, and a national security paradigm. To address the major policy problems identified and framed by different conceptualizations, these paradigms strive to provide legal prescriptions and enforcement tools, enabling the Big Three to institutionalize their preferences underlying cross-border data flows.

A. A Trade Paradigm to Regulate TPDF

The economic conceptualization of personal data paves the way for a trade paradigm to govern TPDF. Currently, the U.S. takes the lead in advancing this approach in the international regulatory arena. Highlighting the economic value of personal data for the digital economy and technological innovation, this paradigm represents an economic approach of regulation, focused on maximizing the economic efficiency and minimizing the transaction costs of TPDF.

(A) The Underlying Economic Logic

From the perspective of this trade paradigm, governments' regulatory intervention should focus on promoting free data flows across borders and disciplining domestic measures that hinder such flows. Since personal data has become an important input for transnational trade, commerce flows, and the data-driven economy, domestic measures that restrict TPDF may constitute non-tariff trade barriers.[180] Therefore, international trade agreements should ensure unrestricted cross-border data transfers by default, and regulate disguised forms of "digital protectionism".[181]

---

[178] Chander & Sun, *supra* note, 10. For a detailed discussion of "data sovereignty", see *infra* chapter 5 ("China's Data Sovereignty"), section I.C.

[179] see *infra* chapter 5 ("China's Data Sovereignty"), section II.A.

[180] Yakovleva, *supra* note, 465, 469-474. See e.g., United States Trade Representative, *Fact Sheet on the 2020 National Trade Estimate: Strong Binding Rules to Advance Digital Trade*, March 2020, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade (noting that key barriers to digital trade include various foreign governments' data localization requirements).

[181] 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*, 14 WORLD TRADE REV. 671, 674 (2015)

First, unrestricted cross-border data flows are essential to international trade. In the digital economy, personal data has become "a core input factor" in the production of digital services, smart products, production processes, targeted advertisements, marketing, and logistics.[182] Domestic measures restricting TPDF would decrease imports of digital services,[183] undermine the efficiency in multinational firms' global production and supply of services and goods, and disrupt international trade flows.[184]

Second, domestic measures that restrict cross-border data flows would also increase the costs of conducting business for multinational corporations,[185] and place foreign digital service providers at a less favorable position, compared with their domestic competitors that need not handle such restrictions. This can create an uneven playing field favoring a host state's domestic tech firms and digital industry.[186]

Third, given that personal data constitutes "an important ingredient of (AI)-systems and algorithms", domestic data restrictive measures may constrain the aggregation of personal data on a global level, break up the integrated information infrastructures of a global Internet, and thus hamper the development of data-driven technologies.[187]

Following the normative benchmark of economic efficiency, the default rules of international trade agreements should enable cross-border data flows as far as possible, and remove domestic regulatory hurdles at odds with that. Any domestic measures constraining free data flows could constitute undesirable digital trade barriers—unless otherwise justified—and accordingly shall be reduced to a minimal.[188] In contrast, privacy and security represent the limited exceptions, as opposed to the rules themselves: state should intervene to exercise protective power against these

---

(citing USITC, and defining "digital protectionism" as "barriers or impediments to digital trade, including censorship, filtering, localization measures, and regulations to protect privacy"). JAMES STAMPS ET AL., U.S. INT'L TRADE COMMISSION, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, Part 1, at 5–1 to 5–2 (2013), https://www.usitc.gov/publications/332/pub4415.pdf.

[182] JACQUES CRÉMER, YVES-ALEXANDRE DE MONTJOYE & HEIKE SCHWEITZER, COMPETITION POLICY FOR THE DIGITAL ERA 73 (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. See Section II.A.

[183] Martina Francesca Ferracane & Erik van der Marel, *Do Data Policy Restrictions Inhibit Trade in Services?*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (October 2018), DIGITAL TRADE ESTIMATES WORKING PAPER NO. 2, 2018, https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf.

[184] Martina F. Ferracane & Erik van der Marel, *The Cost of Data Protectionism*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (October 2018), https://ecipe.org/blog/the-cost-of-data-protectionism/.

[185] *Id.* These measures would force multinational companies to spend more compliance costs as well as greater costs to establish local data centers in the host state. In contrast, unrestricted transnational information flows enable such firms to "operate globally with less of a physical presence." Yakovleva, *supra* note, 472-473.

[186] Lucas Bergkamp, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER L. & SECURITY REV. 31, 39 (2002).

[187] Yakovleva, *supra* note, 473. Anupam Chander & Uyen P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2014). U.S. CHAMBER OF COMMERCE & HUNTON & WILLIAMS LLP, BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY 2-3 (2014), https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf (warning of a global "splinternet" and resultant economic stagnation.)

[188] Yakovleva, *supra* note, 469-475.

threats only when the market malfunctions. As such, privacy and security are framed as a "necessary evil", serving to ensure that trade works for the general good as a default setting.

Under this trade paradigm, international trade institutions—most notably, preferential trade agreements (PTAs)—should establish legal prescriptions to govern TPDF. In that regard, the U.S. has been a leading actor to champion a trade-based approach, pushing for digital trade rules to ensure unrestricted cross-border data transfers. While the WTO negotiations have long been caught in a stalemate and remain unable to bear meaningful fruit thus far, the U.S. has been shifting the rule-making process from the multilateral forum to PTAs, shaping the emerging regulatory standards based on its economic-oriented preferences.[189]

(B) Mega-Regional Trade Agreements

At the international level, the U.S. has been advancing international trade agreements to regulate TPDF, exemplified by post-WTO mega-regional PTAs. Unlike previous PTAs, the Trans-Pacific Partnership (TPP) and United States Mexico Canada Agreement ("USMCA") have incorporated binding and enforceable provisions to ensure free data flows across borders.[190] Treating these high-standard digital trade rules as a priority for its trade policy, the U.S. has been advancing these legal prescriptions at the WTO forum and during its subsequent PTA negotiations.[191]

1. Free-Data-Flows Provisions

First, both TPP and USMCA contain a legally binding and judicially enforceable provision to promote free data flows, requiring that member states "shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."[192]

Notably, this horizontal "free-data-flows" provision addresses "data localization" measures—both *de jure* (that legally require foreign digital firms to store and process data in the host state) and *de facto* (that incentivize localized data storage and processing by enforcing stringent restrictions on cross-border data flows).[193] By design, such a provision imposes a sweeping and binding obligation for member states to guarantee unrestricted cross-border transfers of information (including personal data). Failing that, other treaty parties may bring claims to the state-state

[189] For a detailed discussion of this process of "vertical forum-shifting", see *infra* chapter 2 ("U.S.-Led Regime- and Forum-Shifting"), section IV.

[190] Despite the Trump administration's withdrawal from TPP, these digital trade provisions were incorporated in the final text of Comprehensive and Progressive Agreement for the Trans-Pacific Partnership ("CPTPP") concluded without the US, as well as in the USMCA (a 2.0 version of NAFTA).

[191] Yakovleva, *supra* note, 489-490. See USTR, *Fact Sheet on U.S.-Japan Digital Trade Agreement*, October 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement.

[192] TPP, art. 14.11.2.

[193] Thomas Streinz, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, in MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP 312, 332 (Benedict Kingsbury et al. eds., 2019). Re *de facto* data localization measures, see also Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771, 772, 777 (2020) ("By 'soft data localization,' I mean a legal regime that puts pressure on companies to localize, not by directly requiring localization of data or processes, but by making alternatives legally risky and thus potentially unwise.").

dispute settlement mechanism under the treaty, potentially resulting in economic sanctions to ensure compliance.[194]

As an exception, member states may implement measures that restrict cross-border data flows to achieve legitimate public policy objectives.[195] But to invoke this carve-out, the disputed measures must not be "applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade" (i.e., the non-arbitrariness/discrimination requirement), and shall not "impose restrictions on transfers of information greater than are required to achieve the objective" (i.e., the necessity requirement).[196] As such, although this exception clause leaves some leeway for regulatory autonomy, it shifts the burden to a host state to defend its data restrictive measures as non-protectionist (and hence legitimate under the treaty).

To begin with, domestic regulatory measures to protect data privacy are structured as an exception, departing from the default rules of unrestricted personal data flows. This makes the privacy value of personal data subordinated to the economic interests generated by free data flows, and places regulations to protect data privacy in a *priori* defensive position to be otherwise justified by the host state.[197]

Notably, when challenging a measure restricting cross-border data flows, a claimant state needs not prove the element of discrimination—whether discriminatory intent or effect, *de jure* or *de facto*.[198] This makes it easier and more probable for the claimant to prevail, compared with the non-discrimination standards (national treatment or most-favorable-treatment clauses) of the GATS and pre-TPP PTAs, which generally require a showing of discrimination.[199] In contrast, under TPP, the burden shifts to the host state to prove that the regulation is not "a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade".[200]

Further, to successfully invoke this exception, a host state should also satisfy an objective "necessity" test, which is designed to scrutinize the relationship between the means and the goals of its measures at issue.[201] Importantly, this "necessity" test does not require a showing of the host state's regulatory intent per se. On that note, USMCA further clarifies that a domestic regulation cannot satisfy this condition "if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service supplier of another Party."[202] This clarification not only emphasizes the economic effects of the measures on the competitive opportunities of foreign digital service suppliers, but also rebuts a presumption that *cross-border* transfers of data per se impose greater risks to the host state's legitimate public policy goals than *domestic* data flows. In this way, it would tilt the balance further in favor of free data flows as a default position, imposing greater constraints on states' regulatory autonomy to adopt measures that hamper TPDF.

---

[194] TPP, arts. 14.18, 28.7, 28.12, 28.19, 28.20.
[195] TPP, art. 14.11.3
[196] *Id.*; USMCA, art. 19.11.2.
[197] Yakovleva, *supra* note, 427.
[198] *Id.*, 497.
[199] *Id.*
[200] TPP, art. 14.11.3.a.; USMCA, art. 19.11.2.a.
[201] TPP, art. 14.11.3.b.; USMCA, art. 19.11.2.b.
[202] USMCA, art. 19.11.2.b (fn.5).

Finally, while some commentators were concerned that this untested provision can result in uncertainties which may water down some states' commitments to free data flows, such uncertainties are arguably a double-edge sword, and could also generate "regulatory chill", thus inhibiting a government from restricting free data flows.[203] If coupled with the USTR's active invocations of domestic trade tools (most notably, section 301 or super 301 investigations, and economic sanctions), this latter risk becomes even more pressing for a less developed country with a modest domestic economy.

2. Provisions Against "Computer Localization"

Second, both TPP and USMCA contain a provision that prohibits the "computer localization" requirements—a particular form of *de jure* "data localization" measures. Under this provision, a member state must not require a person to "use or locate computing facilities"—including "computer servers and storage devices for processing or storing information for commercial use"—in its territory "as a condition for conducting business" there.[204] As such, a host state is disallowed to compel foreign digital companies to localize data storage and processing by requiring the mandatory use of local computing facilities.[205]

In TPP, this "computer localization" provision is subject to an exceptions clause, which adopts the same language of the carve-out from the free-data-flows provision.[206] Although a host state may attempt to invoke the public policy grounds of data privacy protection, cybersecurity, law enforcement, and domestic digital industry development to justify such localization measures, "computer localization" measures have been commonly viewed as "ineffective, unnecessary, and unsustainable" to achieve each of these goals.[207] If a necessity nexus between the means and ends is lacking, it is difficult for such localization measures to survive the scrutiny of this provision. In contrast, USMCA further sharpens this rule by removing the exception clause altogether.[208]

3. Subjecting Measures Restricting TPDF to Investor-State Treaty Arbitration

Moreover, both TPP and USMCA explicitly specify that a state's obligations for free data flows and against data localization are subject to the provisions of the investment chapters.[209] Thus, a foreign investor may bring an investor-state treaty arbitration to challenge data restrictive measures for violating substantive investment protection standards.[210] This means that even if a host state could invoke exception clauses in the e-commerce/digital trade chapter to justify its measures in state-state proceedings, those measures may still have to be scrutinized under investment protection obligations (e.g., anti-expropriation, fair and equitable treatment, or national treatment

[203] Streinz, *supra* note, 332.
[204] TPP, arts. 14.13.2, 14.1. USMCA, arts. 19.12, 19.1.
[205] Streinz, *supra* note, 333.
[206] TPP, art. 14.13.3.
[207] Streinz, *supra* note, 333-334. See Chan-Mo Chung, *Data Localization: The Causes, Evolving International Regimes and Korean Practices*, 52 J. WORLD TRADE 187 (2018); Chander & P. Lê, *supra* note, 713-39.
[208] USMCA, art. 19.12.
[209] TPP, art. 14.2(4)-(5); USMCA, art. 19.2(4).
[210] See, TPP, chapter 9 (investment); USMCA, chapter 14 (investment).

provisions).[211] This double-barreled approach to enforcement (through state-state and investor-state dispute settlement mechanisms) expose a host state to the risks of both trade sanctions and pecuniary compensations, further constraining its regulatory autonomy to depart from the default rules of free data flows.

4. Setting a Permissive Floor on Consumer Protection to Facilitate TPDF

Finally, under an instrumental approach to privacy and data protection, both TPP and USMCA seek to establish a permissive international floor of data privacy standards, thereby removing national regulatory restrictions and facilitating cross-border data flows.[212]

On data privacy protection, TPP treats the mere presence of a domestic legal or regulatory framework to protect the personal data of e-commerce users as sufficient.[213] Thus, almost any form of domestic data privacy regulations may satisfy this obligation, including "comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy".[214] Allowing no review of the substance of a domestic framework, this permissive requirement starkly contrasts with the treaty's high-standard protection for free data flows and its strict scrutiny over domestic measures that restrict data exports.[215]

USMCA adopts the same language of this provision, but adds a reference to the APEC Privacy Framework, the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) (2013 OECD Guidelines), as well as key principles of privacy and personal data protection.[216] It also requires that "any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented."[217] Further, USMCA recognizes the APEC Cross-Border Privacy Rules (CBPR) system as "a valid mechanism to facilitate cross-border information transfers while protecting personal information."[218] Unlike the EU's fundamental rights approach, these regional and international instruments embody an economic approach to privacy and data protection, treating data privacy standards as an instrument to enhance consumer confidence in e-commerce and to facilitate digital trade.[219]

---

[211] Andrew Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH 182, 230 (2017) (noting that a host state "would then need to demonstrate that its conduct did not breach an investment protection obligation, or to rely on an alternative exceptions clause, such as the security exception in TPP art. 29.2").
[212] Aaronson, *supra* note, 19. Streinz, *supra* note, 334 (noting that the TPP establishes "only a privacy floor"). Regarding this instrumental view of privacy and data protection, see eg., TPP, art. 14.8.1; USMCA, art. 19.8.1 ("The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the *contribution that this makes to enhancing consumer confidence in digital trade*.") (emphasis added).
[213] TPP, art. 14.18.2.
[214] *Id.* (fn.6).
[215] Streinz, *supra* note, 334.
[216] USMCA, art. 19.8.2-3.
[217] *Id.*, art. 19.8.3.
[218] *Id.*, art. 19.8.6.
[219] Yakovleva, *supra* note, 492. LEE ANDREW BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 76 (2014).

(a) OECD Guidelines

Different from the General Data Protection Regulation ("GDPR"), the OECD Guidelines only establish a set of minimum standards on data privacy protection.[220] Driven by the economic concerns that domestic privacy regulations may pursue protectionist goals,[221] the Guidelines primarily aim at promoting free data flows and minimizing domestic restrictions on data exports.[222] In terms of substantive data governance, the standards of the Guidelines are based on the "accountability principle", which requires a data controller to remain "accountable for complying with measures which give effect to" the core data privacy protection principles.[223] Under the accountability principle, a data controller should set "a privacy management programme" to provide "appropriate safeguards based on privacy risk assessment", and give notice to inform regulatory authorities and/or affected data subjects of significant security breaches.[224] While the Guidelines primarily rely on data controllers to carry out the core protection principles, they are not very prescriptive with respect to how firms should implement these standards—neither have they specified in detail the supervisory role of national governments in ensuring compliance.[225] In essence, this model of data privacy protection represents a market-based approach with minimalist regulatory intervention, primarily relying on business self-regulation.

Regarding cross-border data flows, the Guidelines reiterate the "accountability principle", obliging a data controller to "remain accountable for personal data under its control without regard to the location of the data."[226] Further, the Guidelines generally require a member state to "refrain from restricting (TPDF) between itself and another country", provided that the receiving country substantially complies with these Guidelines, or the data controller implements "sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures…. to ensure a continuing level of protection consistent with these Guidelines."[227] Notably, this provision replaces a more onerous "equivalent domestic data privacy legislation" requirement

---

[220] 2013 OECD Guidelines, para. 6.

[221] Michael Kirby, *Legal Aspects of Transborder Data Flows*, 5 INT'L COMPUTER L. J. 233, 237 (1991) (the author, who headed the expert group in charge of drafting the original OECD Guidelines, commented that: "It was the fear that local regulation, ostensibly for privacy protection, would, in truth, be enacted for purposes of economic protectionism, that led to the initiative of the OECD to establish the expert group which developed its Privacy Guidelines."). Id., Chapter 4, The Evolving Privacy Landscape, at 126 (fn. 120) ("Under Recommendations, the Guidelines state, 'That Member countries endeavour to remove, or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data'.").

[222] Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, 17 WORLD TRADE REV. 477, 484 (2018) (noting that "(the) 2013 revision subordinated the regulation of transborder flows of personal data to economic needs even more than the previous set by adopting a risk-based approach."). See 2013 OECD Guidelines, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, Council Recommendation ("The Council… DETERMINED to further advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among them.").

[223] 2013 OECD Guidelines, para. 14.

[224] *Id.*, para. 15.

[225] Regarding the Guidelines' encouragement of self-regulation, see *id*., para. 19 (d)(g) (National Implementation: "Member countries should… encourage and support self-regulation, whether in the form of codes of conduct or otherwise… consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy.").

[226] Id., para. 16.

[227] Id., para. 17.

(from the 1980 version) with a criterion of "substantial consistency with the Guidelines", which seemingly narrows the grounds for a state to restrict cross-border personal data flows.[228] Further, since the Guidelines generally are not very prescriptive and establish a relatively low level of data privacy protection,[229] their requirements on free data flows can be more easily met by a recipient country or data controllers, compared with the stringent rules of the GDPR.

(b) APEC Privacy Framework and CBPR system

Modelled on the OECD Guidelines, the APEC Privacy Framework is an international instrument aimed primarily at promoting e-commerce and trade flows.[230] In its preamble, its rationale is predominantly based on economic concerns—to prevent commercially adverse restrictions on cross-border personal data flows and to boost consumer confidence in e-commerce—compared with human rights concerns.[231] As such, the Framework largely views privacy and data protection as a matter of consumer protection, which is not so much intrinsic human rights as an economic necessity to promote digital trade.[232] Substantively, the Framework comes with "a mild prescriptive bite".[233] Although its data privacy standards (crystalized in a set of "Information Privacy Principles")[234] are consistent with the core principles of the OECD Guidelines, the Framework's protection standards are generally lower than those of the EU Data Protection Directive or GDPR.[235]

As for the regulation of data exports, the Framework does not explicitly allow states to restrict cross-border transfers of personal data to jurisdictions with a weaker level of data protection.[236] Rather, like the OECD Guidelines, the Framework's TPDF rules are based on a general principle of "accountability", which holds data collectors accountable for complying with the original data

---

[228] See OECD Guidelines 1980, para. 17 (permitting a member state to restrict TPDF in case of "certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides *no equivalent protection*." (emphasis added). See Bygrave, *supra* note, 48.

[229] Yakovleva, *supra* note (WTR), 485.

[230] See APEC Privacy Framework 2015, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015), preamble, para. 5 ("The Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's Guidelines…").

[231] Bygrave, *supra* note, 75-76. APEC Privacy Framework 2015, preamble, paras. 1 ("Consumer trust and confidence in the privacy and security of online transactions, information networks and management of personal information is critical in enabling member economies to reap the benefits of electronic commerce and participate in today's information-driven economy"), 3 ("Regulatory systems that unnecessarily restrict this flow or place burdens on it have adverse implications for global business, economies and individuals. Therefore… there is also a need to develop systems for protecting privacy that account for these realities in the global environment.").

[232] Bygrave, *supra* note, 76. See eg., APEC Privacy Framework 2015, preamble, paras 1 ("APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce and innovation must be cooperation to promote both effective information privacy protection and the free flow of information in the Asia Pacific region, while respecting domestic (privacy) laws and regulations…"), 2 ("there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and businesses.").

[233] Bygrave, *supra* note, 76.

[234] APEC Privacy Framework 2015, Part III Principles, paras. 19-32.

[235] BYGRAVE, *supra* note, 76 ("For instance, the Framework does not embrace the sensitivity principle, and it applies the criteria of 'fair' and 'lawful' only to the *collection* of personal information… as opposed to further stages of information processing as well."). See eg., *id.*, Principle III, paras. 22.

[236] BYGRAVE, *supra* note, 77.

protection framework, irrespective of the location of a data recipient country.[237] As such, the Framework largely relies on the market mechanisms to protect individuals' data privacy.

Designed to enforce the principles of this Framework, the APEC CBPR system is a voluntary certification scheme to protect data privacy for cross-border data transfers.[238] Following the certification by a government at the country level (i.e., a "participating economy"), domestic firms may apply for certification from an independent accountability agent, the issuance of which is meant to demonstrate their internal data privacy policies and practices comply with the APEC Privacy Framework.[239] CBPR-certified companies are allowed to freely transfer personal data among participating economies. Compared with the GDPR, the CBPR is generally much less prescriptive (on data privacy protection) and restrictive (as to TPDF), and thus is deemed more conductive to facilitating cross-border data flows.[240] The U.S. promotes the CBPR as a better regulatory model than the EU's GDPR for cross-border data transfers, and pushes for new-generation PTAs that recognize the CBPR as a valid mechanism to protect personal data in transit.[241]

(c) Preventing Regulatory Overkill

Having established relatively permissive standards of data privacy protection, USMCA's digital trade chapter further stipulates a recognition that "any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented."[242] Aimed at preventing regulatory overkill and minimizing compliance costs for firms, this provision would further constrain the autonomy of states to regulate data privacy protection. Under the prevailing economic rationale, internal measures of data privacy protection are justified only to the extent necessary to maintain and preserve consumers' trust in e-commerce and digital trade.[243]

****

[237] APEC Privacy Framework 2015, Principle IX, paras. 32 ("A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."), 69-70.
[238] APEC, *What Is the Cross-Border Privacy Rules System?*, Fact Sheets (April 15, 2019), https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system.
[239] *Id.*
[240] Clare Sullivan, *EU GDPR or APEC CBPR? —A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era,* 35 COMPUTER LAW AND SECURITY REVIEW 380, 381 (2019).
[241] *Id.* See APEC Electronic Commerce Steering Group, APEC Cross-Border Privacy Rules System Goes Public, Press Release (July 31, 2012), https://www.apec.org/press/%20news-releases/2012/0731_cbpr.aspx (as commented on by the then US Federal Trade Commissioner Edith Ramirez, "We hope that many more APEC economies will soon join and help realize the system's potential as a model for global interoperability among privacy regimes."). See e.g., USMCA, art. 19.8.6; USTR, *Fact Sheet on U.S.-Japan Digital Trade Agreement*, *supra* note.
[242] USMCA, art. 19.8.3.
[243] Yakovleva, *supra* note (Privacy Protectionism), 510.

Undergirded by a dominant economic conceptualization of personal data, the U.S.-led trade paradigm approaches data privacy protection as a precondition for digital trade and as an economic necessity,[244] rather than intrinsic human rights values that are able to trump competing economic considerations in their own right. Under this trade paradigm, data privacy protection largely becomes a matter of consumer welfare anchored in the commercial sphere, which is not so much valuable in its own right as for its capabilities to boost e-commerce, digital trade, and technology innovation.[245] In this light, the privacy value of personal data is redefined as an ancillary, subordinated trade interest, serving an instrumental function to promote commerce flows.[246] This regulatory approach generates two far-reaching policy implications.

First, domestic regulations to protect data privacy are framed as potential digital trade barriers—at least to the extent that they may result in adverse trade effects and undercut economic efficiency. In this way, these regulations are placed in a defensive position *a priori*, and must justify their legitimacy under an objective "necessity" test. Second, individuals' data privacy protection is largely relegated to the market mechanisms, particularly digital firms' self-regulation and voluntary certification. Focused on "protecting consumers in a data marketplace", this trade paradigm seeks to transplant the U.S.'s *domestic* approach to information privacy regulation to the *international* level.[247]

In short, by establishing a permissive international privacy floor and restraining states' regulatory autonomy, this economic approach to data privacy protection strives to keep regulatory barriers to TPDF to a minimum, paving the way for maximizing data's economic interests.

B. A Fundamental Rights Paradigm to Regulate TPDF

Different from the economic framing, the rights-oriented conceptualization of personal data justifies a fundamental rights paradigm to govern TPDF. Thus far, the EU leads the way in advocating a rights-based regulatory approach, addressing cross-border transfers of personal data as a matter of fundamental rights protection. Prioritizing the privacy value of data, this approach focuses on ensuring adequate data protection as a key criterion for allowing outbound personal data transfers.

(A) The Underlying Fundamental Rights Logic

Under the fundamental rights paradigm, safeguarding data privacy is an overarching objective in the regulatory design. Accordingly, TPDF regulation focuses on adequate protection of personal data against foreign private and public-sector actors (surveillance capitalism and the surveillance state) as a normative priority, ensuring the inviolability of fundamental rights.[248]

---

[244] *Id.*, 492.
[245] *Id.*, 514. See BYGRAVE, *supra* note, 76.
[246] Yakovleva, *supra* note, 492.
[247] *Id.* See Schwartz & Peifer, *supra* note, 115
[248] See Schwartz & Peifer, *supra* note, 145. See also SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (PUBLIC AFFAIRS 2019).

Such a fundamental logic generates two major implications for the institutional design of this legal paradigm. First, privacy and data rights are just too important to be left to the market mechanisms to regulate. As noted earlier, normatively, personal data, as an embodiment of fundamental rights, should not be easily traded like a commodity in the market; and the fundamental rights of data subjects are only partially alienable.[249] Given the unbalanced power relationship between an individual data subject and a data controller (whether private or public), relying primarily on the market mechanisms and business self-regulation not only may prove inadequate to ensure a sufficient level of data protection, but also can exacerbate the existing imbalance of power.[250] Thus, instead of embracing an economic approach, legislators and policymakers should advance a rights-based paradigm, focused on high-standard protection of data privacy as a normative priority.

Following this logic, neither the PTAs nor the market mechanisms—both characterized by an economic approach to data privacy protection—are the appropriate institutions to provide the legal and regulatory solutions for TPDF. This explains why the EU adopts a relatively cautious approach to digital trade negotiations: thus far, the EU has incorporated no binding provisions on TPDF in its PTAs, thereby ensuring its unchallenged regulatory autonomy to safeguard data privacy as fundamental rights.[251]

In its model provisions on free cross-border data flows and personal data protection (to be included in trade and investment treaties), the EU not only recognizes rules on TPDF as valid regulatory tools to protect privacy data, but also adopts a self-judging styled exception to immunise "the safeguards it deems appropriate to ensure the protection of personal data and privacy" from international adjudication under the treaty.[252] Aligned with art. XXI (national security exception) of the GATS, this exception clause features a "subjective necessity" test, contrasting with the "objective necessity" test in the equivalent provisions of TPP and USMCA.[253]

In addition, unlike TPP or USMCA that subjects any measures restricting TPDF to investment protection obligations, the EU's model provisions also specify that the investor-state dispute

---

[249] See *infra* Section II.B.

[250] If private-sector actors obtain excessive power with respect to personal data, this could eventually translate into the government's unchecked authority and capacity vis-à-vis individuals (as public authorities may obtain those data through intelligence surveillance, domestic laws, or otherwise), thereby further undermining the normative goals of protecting individuals' human rights, personal dignity, and self-autonomy.

[251] Steinz, *supra* note, 334 (observing that the EU insisted not to negotiation provisions on privacy and data protection in Transatlantic Trade and Investment Partnership and Trade in Services Agreement); Yakovleva, *supra* note (Privacy Protectionism), 493 (noting in the EU-Japan PTA and EU-Mexico PTA, the EU expressly refrained from containing provisions on free TPDF; instead, they both included a three-year review clause to allow both parties to reconsider this issue later).

[252] Horizontal Provisions on Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements) ("Horizontal Provisions"), Article B, para. 2, https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf ("Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards."). Yakovleva, *supra* note (Privacy Protectionism), 494-496 (noting that these model provisions have been incorporated into "currently negotiated trade agreements with New Zealand, Australia, Chile, Indonesia, and Tunisia, and in (EU's) proposal for the recent WTO negotiations on electronic commerce").

[253] Yakovleva, *supra* note (Privacy Protectionism), 496. See TPP, art. 14.11(3); USMCA, art. 19.11(2); GATs, art. XXI.

settlement mechanism (i.e., investment court system) does not apply to measures on cross-border data flows and to protect personal data and privacy.[254] As such, while the U.S.-led economic approach to TPDF addresses domestic measures restricting TPDF as "digital trade barriers" and mistreatment of foreign investors, the EU seeks to guarantee that domestic regulations for privacy and data protection do not constitute "digital protectionism" or internationally wrongful acts on foreign investments, irrespective of any potentially adverse impacts on cross-border data flows.[255]

Instead, the EU deploys a fundamental rights paradigm to regulate TPDF. Substantively, this legal paradigm is characterized by high-standard protection of personal data and privacy as fundamental rights, as well as a "prohibition subject to limited exceptions" approach to TPDF.[256] Institutionally, the decision-making authority to govern TPDF largely belongs to regulatory institutions devoted to data privacy protection (including national data protection authorities (DPAs) and European Data Protection Board ("EDPB")), as well as supranational and domestic judiciaries entrusted with safeguarding fundamental rights (e.g., the European Court of Justice ("ECJ"), national courts).

Second, given that data may be transmitted worldwide via cyberspace in an almost frictionless fashion, strong data privacy protection would be of no avail if the laws readily lose their legal effects beyond national borders.[257] If unaddressed, this "territoriality" limitation of data protection law could make for easy circumvention by transborder data operators, creating gaping loopholes that may doom the efficacy of its rules. Therefore, regulations should ensure that under certain conditions, data protection rules attach to domestic personal data transmitted overseas.[258]

Given that the EU accords great significance to the privacy value of personal data, its data protection regulation is designed to have strong extraterritorial effects. This not only enables European data protection law to follow the personal data of EU-based individuals (regardless of where that information flows),[259] but also grants national and EU-level regulatory authorities a "data embargo power", capable of blocking data exports to jurisdictions whose data privacy protections fall short of EU standards.[260]

(B) Protection of Privacy and Personal Data as Fundamental Rights

At the core, this European fundamental rights paradigm has been implemented through the EU Data Privacy Directive 95/46/EC ("DPD") and the succeeding GDPR. Meanwhile, it has been squarely anchored in the broader European constitutional structures.

At the statutory level, individuals' privacy and personal data are currently protected by the GDPR, an omnibus data protection legislation. Unlike its predecessor—the DPD, which required national legislation for implementation—the GDPR is a binding, enforceable regulation. This departs from

[254] Horizontal Provisions, Article B, para. 4.
[255] Yakovleva, *supra* note (Privacy Protectionism), 465-466.
[256] See *infra* section III.B.(B)-(C).
[257] Paul Schwartz, *Global Data Privacy—The EU Way*, 94 NYU L. R. 771, 783 (2019).
[258] *Id*.
[259] See e.g., GDPR, art. 3 (detailing the GDPR's scope of extraterritorial application).
[260] Schwartz, *supra* note (EU Way), 778, 783; Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1984 (2013).

the traditional trajectory of EU consumer protection law that usually enacts directives (rather than regulations) to protect individuals, evincing the fundamental rights nature of data protection.[261]

Substantively, the GDPR provides a comprehensive set of individual rights, basic principles governing the processing of personal data, as well as corporate data governance duties on digital firms (irrespective of whether individuals invoke their rights).[262] Compared with the DPD, the GDPR is more comprehensive, prescriptive, and stringent. Not only does the GDPR sharpen the bite of existing data protection rights (such as the "right to be forgotten"),[263] but it also creates new rights for data subjects,[264] new obligations for digital firms,[265] higher sanctions,[266] as well as stronger enforcement mechanisms (e.g., a new class-action styled remedy).[267]

Further, the GDPR's provisions feature strong enforceability, reflecting the high status of data subjects in the fundamental rights paradigm. For instance, this regulation grants data subjects the "right to an effective legal remedy against a controller or processor",[268] and has facilitated the legal avenues for individuals to bring claims. Where a data subject suffered "material or non-material damage" due to a breach of the regulation, she is entitled to claim compensation, including damages for emotional distress and pain even short of monetary loss.[269] An individual may also mandate a NGO to make claims for compensations on her behalf, or make a complaint with a data protection supervisory authority.[270]

At a deeper level, privacy and data protection are firmly anchored in European constitutional structures, which use the language of human rights to protect data subjects, safeguarding their personhood and self-autonomy against potential risks caused by data processing.[271]

The right to privacy—which has long been recognized in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights—was stipulated as a human right in the European Convention on the Protection of Human Rights and Fundamental Freedoms (ECHR).[272] The right to the protection of personal data, though not explicitly provided in the ECHR, has been incorporated into the right to a private life through the ECtHR's judicial interpretations.[273] With common roots in international and regional human rights laws, both rights

---

[261] Schwartz & Peifer, *supra* note, 128-129.
[262] See generally, the GDPR, chapter 2 to 4. See also Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. R. 93, 98 (2021).
[263] See e.g., GDPR, art. 17 (strengthening the ability of a data subject to erase her personal data).
[264] See e.g., GDPR, art. 18 (a right of "data portability").
[265] See e.g., GDPR, arts. 22 (a general duty of accountability on data controllers), 31-32 (a new obligation on data controllers to notify data subjects and DPAs of "personal data breaches"), 35 (new duties on data controllers and processors to appoint internal "data protection officers").
[266] See e.g., GDPR, art. 83(5) (allowing fines up to four percent of a firm's global revenue or 20 million Euros, whichever higher).
[267] See e.g., GDPR, art. 80.
[268] GDPR, art. 79.
[269] GDPR, art. 82. See EU General Data Protection Regulation—Key Changes, DLA Piper (Press Release), https://www.dlapiper.com/en/us/focus/eu-data-protection-regulation/key-changes/.
[270] GDPR, arts. 77, 80.
[271] *Id*., 127.
[272] ECHR, art. 8; see UDHR, art. 12; ICCPR, art. 17.
[273] D. HARRIS ET AL., LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 362 (OUP, 2009). See ECHR, art. 8.

were also recognized as two fundamental rights in the EU Charter of Fundamental Rights (in articles 7 and 8, respectively), constituting the constitutional principles in EU primary law.[274]

With respect to personal data protection, article 8 of the EU Charter of Fundamental Rights lays out a set of key fair information practices (which the DPD and GDPR were based on): "(1) a requirement of fair processing; (2) a requirement of processing for specified purposes; (3) a requirement of consent or other legitimate basis for processing; (4) a right of access to data; (5) a right to have data rectified; and (6) a requirement of independent data protection authorities checking compliance with these rules."[275] Further, the Treaty on the Functioning of the European Union, which forms the constitutional foundation of the EU, also explicitly provides the right to the protection of personal data.[276]

At the member states level, the right to protection of personal data has been recognized as a constitutional right in a number of EU countries, whether through explicit constitutional text or judicial interpretations.[277]

Importantly, recognizing privacy and data protection as fundamental rights has three major normative consequences. First, it bolsters the normative status of data privacy protection in the EU legal system (including the GDPR and other sectoral EU laws), reinforces the level of protection for data subjects, and makes violations of data protection norms "more readily sanctioned".[278]

As is common for European constitutional rights, the rights to privacy and data protection not only constrain the governments, but also apply to "private-on-private" relations—most notably—between individual data subjects and private-sector data controllers and processors.[279] In addition, as fundamental rights, individuals' privacy and data protection should be protected even absent a specific harm to the individual or her sensitive data.[280] As stated by the ECJ stated in *Schrems*, "(t)o establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question … is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference."[281] Instead, given that the processing of personal data imposes an inherent threat to data subjects, such a processing activity is allowed only if the law permits so.[282] And when personal data is abused or

[274] EU Charter of Fundamental Rights, arts. 7, 8. Termed the European "Bill of Rights", the EU Charter of Fundamental Rights has the highest legal force in EU law. See Yakovleva, *supra* note (WTR), at 486.
[275] Schwartz & Peifer, *supra* note, 128. See EU Charter of Fundamental Rights, art. 8.
[276] Treaty on the Functioning of the European Union, art. 16.
[277] *Id.* (these countries include "Germany… Czech Republic, Greece, Hungary, Lithuania, Poland, and the Slovak Republic, and Spain"; for instance, Germany recognized the "right to informational self-determination in 1983 and the "right of trust and integrity in information systems" in 2008).
[278] Bygrave, *supra* note, 59 (noting such a trend from the recent developments of ECJ jurisprudence).
[279] Schwartz & Peifer, *supra* note, 126.
[280] Schwartz & Peifer, *supra* note, 127.
[281] *Schrems,* 2015 E.C.R. 650 at para. 87. Likewise, the ECJ noted in *Google Spain* that the fundamental interests of data subjects do not hinge on whether the processing of the personal data at issue "causes prejudice to the data subjects." See *Google Spain*, 2014 E.C.R. 317, para. 96.
[282] Schwartz & Peifer, *supra* note, 127.

misused, the legal protection follows the harms to a data subject, and does not hinge on an injury to the individual's economic/material interests.[283]

Further, the fundamental rights nature of privacy and data protection also makes derogations from these norms "more difficult".[284] Under the EU Charter of Fundamental Rights, if the fundamental rights and freedoms were to be limited, such restrictions "must be provided for by law" (such as a statutory provision), and must ensure that the essence or the core part of such rights are "free from alteration or intrusion, whether through legislation or other means."[285] Meanwhile, it is the EU's judiciary that is entrusted with the important mandate "to identify and safeguard the essence of the Charter's rights."[286]

Second, since the EU's constitutional system features a plurality of constitutional sources and judicial bodies, protecting the fundamental rights of privacy and data protection could create an "overlap of judicial institutions and governance layers for protecting human rights."[287] The latter include, most notably, national courts (including domestic constitutional courts), national legislatures, national data protection authorities, the ECtHR, and the ECJ. Such an institutional overlap may create "an incentive for an expansion of the norms and institutions for the protection of fundamental rights".[288] Also, it opens the door to national and intra-EU judicial dialogues and inter-institutional exchanges on data privacy protection, which can trickle down into a process that enhances these authorities' shared knowledge, professional expertise, and discursive power.

Third, while the EU also subscribes to the importance of free data flows, the fundamental rights of privacy and data protection typically would prevail over such an interest under a proportionality test.[289] Despite their importance, free information flows do not weigh as much as a fundamental interest in the EU's fundamental rights paradigm.[290] To supersede a fundamental right, it is not sufficient for "the constitutional benefits (to) outweigh the constitutional costs".[291] Rather, under the proportionality test, the question is whether the law's protection of a competing interest could be achieved "at a lower constitutional cost to privacy".[292] This "least-restrictive" test makes it even

---

[283] Schwartz & Peifer, *supra* note, 127, 129 ("Both the data subject and a data protection authority can request an injunction to stop a practice that harms a privacy interest and can receive damages based on a nonmaterial injury in cases of a serious invasion of one's protected sphere of privacy."). Thus, processing personal data without a legal basis is, in and of itself, a violation of data privacy rights. See *id*.

[284] Bygrave, *supra* note, 59.

[285] Schwartz & Peifer, *supra* note, 129. See EU Charter of Fundamental Rights, art. 52(1).

[286] Schwartz & Peifer, *supra* note, 129.

[287] FEDERICO FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE 13-14, 26 (2014).

[288] *Id.* See e.g., EU Charter of Fundamental Rights, art. 52(3) ("In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention (by the ECtHR). This provision shall not prevent Union law providing more extensive protection."), 52(4) ("In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions.").

[289] Schwartz & Peifer, *supra* note, 130-31. See the GDPR, Recital 3 ("Directive 95/46/EC of the European Parliament and of the Council seeks to … ensure the free flow of personal data between Member States."), Recital 4 ("The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.").

[290] Schwartz & Peifer, *supra* note, 131.

[291] ALEX STONE SWEET, GOVERNING WITH JUDGES 98-99 (2000).

[292] Schwartz & Peifer, *supra* note, 131. See id.

more difficult for a competing interest to restrict a fundamental right. When in conflict, free information flows therefore can rarely trump the rights to privacy and data protection.[293]

In any event, in this fundamental rights paradigm, the high level of data privacy protection can be lowered only to the extent necessary to balance competing fundamental rights (or interests) with an equivalent normative weight.[294] Thus, its level of data protection would be higher than that of the economic approach, which seeks to maintain data privacy protection only to the extent necessary to preserve sufficient trust for e-commerce and digital trade.[295]

(C) A "Prohibition Subject to Limited Exceptions" Approach to TPDF

While high-standard protection of privacy and personal data could safeguard fundamental rights *within* the EU, data's inherent mobility could make European data protection law futile, if its application is restricted to its borders. To effectively address this risk, this fundamental rights paradigm is designed to have strong extraterritorial effects, potentially reaching outside the EU's territory. Though controversial, the EU justifies this extraterritoriality by the necessity of protecting fundamental rights.[296]

Unlike the U.S. approach that promotes free data flows, the EU's fundamental rights paradigm places a qualified prohibition on unrestricted transfers of personal data from EU member states to any third countries, unless the latter provide "an adequate level" of data protection.[297] As interpreted by the ECJ, "adequate" refers to an "essentially equivalent" level of data protection, compared with the standards under the EU Charter and DPD (and by implication, the GDPR).[298] In this regard, the European Commission ("Commission") unilaterally assesses the adequacy of a third country's data protection system on a case-by-case basis, taking into account its domestic legal and administrative institutions as well as its international obligations.[299] If positive, the Commission would issue a binding "adequate" decision to permit unrestricted personal data flows to that country.

If not, cross-border transfers of personal data could take place only if the data controllers or processers adopt "appropriate safeguards" (including standard contractual clauses (SCCs), binding corporate rules, the certification mechanism, or codes of conduct) to protect data subjects, granting the latter enforceable rights and effective legal remedies.[300] Aligned with the definition of "adequate" protection, these alternative mechanisms should provide "a level of protection

[293] See Cedric Ryngaert & Mistale Taylor, *Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?*, 114 AJIL Unbound 5, 7 (2020) (noting that the ECJ has, "in a string of well-known rulings with a transatlantic dimension, such as *Schrems*, *Canada-EU PNR*, and *Google Spain*, so strongly emphasized the right to data protection over countervailing interests, such as security and the free flow of information.").
[294] Yakovleva, *supra* note (WTR), at 484.
[295] *Id*. See Section III.A.
[296] Ryngaert & Taylor, *supra* note, 5-7.
[297] GDPR, art. 45; DPD, art. 25.
[298] Case C. 362/14, *Schrems v. Data Protection Commissioner* (*Schrems I*), October 6, 2015, [2015] ECLI:EU:C: 2015:650, para. 73.
[299] GDPR, art. 45(2).
[300] GDPR, arts. 46-47.

essentially equivalent to" that of the GDPR and EU Charter.[301] Such an assessment shall take into account not only the contractual clauses at issue, but also the legal system of the recipient country, for instance, with respect to the pubic authorities' capacity to access and control the transferred data.[302] Among these mechanisms, SCCs are the most often used vehicle to export personal data outside Europe.[303]

In exceptional circumstances, if the data exporters try to use these "appropriate safeguards" but to no avail, they could rely on enumerated derogations as a last resort. The latter include the data subject's explicit consent, or where the transfer is *necessary* (i) for the performance or conclusion of a contract, (ii) for an important public interest, (iii) for pursuing legal claims, or (iv) for protecting the vital interests of the data subject.[304] As for the "contract", "legal claims", "public interest", and "vital interests" derogations, they shall be subject to an necessity test to examine whether the data transfer is necessary for the specific purpose.[305] In particular, the "contract" and "legal claims" derogations could only apply to non-repetitive, occasional transfers, as opposed to massive, systemic transfers.[306] With respect to the "explicit consent" derogation, its invocation should satisfy relatively high thresholds and restrictive conditions, which in turn can make it expensive and time-consuming, and thus may undercut its practical feasibility.[307] In any event, all these derogations must not be construed in ways defeating their very nature (i.e., the narrow exceptions to the default rules of adequate protection, or alternatively, appropriate safeguards).[308]

As such, the EU's rules for outbound personal data transfers are characterized by a "prohibition subject to limited exceptions" approach. This approach is notable in three major aspects. First, as explained by the ECJ, this approach strives to protect Europeans' fundamental rights by preventing circumvention of EU data protection norms through transfers to third countries.[309] Thus, unlike the U.S. that frames the TPDF rules as an economic instrument to promote economic flows, the EU conceptualizes such rules as indispensable regulatory tools to protect fundamental rights as

---

[301] Case C. 311-18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (Schrems II)*, July 16, 2020, [2020] ECLI:EU:C:2020:559, ruling, para. 2.
[302] *Id.*
[303] Chander, *supra* note, at 774 (noting that "a large fraction of data exports from the EU rely on SCCs"). It bears noting that binding corporate rules can only be used for intra-company transfers of data (rather than transfers to third parties), and that to date the EU has not officially provided mechanisms of certifications and codes of conduct. See *id*., at 775, 777.
[304] GDPR, art. 49.
[305] European Data Protection Board, Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679, May 25, 2018, at 5, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf
[306] Id., 4-5. See GDPR, Recital 111.
[307] GDPR, art. 4(11) ("'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"), art. 7 (specifying a set of conditions for consent to be valid). EDPB, Guidelines 2/2018, 2016/679, *supra* note, at 6-8 (giving a restrictive interpretation on the conditions to invoke the "consent" derogation: consent must be explicit, specific, and informed); See Information Commissioner's Office (ICO), *International Transfers After the UK Exit from the EU Implementation Period*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ (according to the ICO, the UK DPA, "Given the high threshold for a valid consent, and that the consent must be capable of being withdrawn, this may mean that using consent is not a feasible solution.")
[308] EDPB, Guidelines 2/2018, 2016/679, *supra* note, at 5.
[309] *Schrems I*, para. 73.

intrinsic, inviolable normative values. At a deeper level, this conceptual difference is rounded in the U.S. and the EU's dominant conceptualizations of personal data (as a digital factor of production, or an embodiment of fundamental rights, respectively).[310]

Second, EU's layered approach to TPDF regulation places the burden on third countries and their companies to comply with European data protection standards, in the shadow of blocking or restricting outbound data transfers. Notably, EU data protection law grants EU authorities a "data embargo power" to block personal data flows to jurisdictions failing to satisfy the EU's data protection standards.[311] Such an embargo power is exemplified in the Commission's "adequacy" decision. Rather than a "one shot" deal, the adequacy finding is subject to the Commission's regular monitoring on an ongoing basis. Upon findings of circumstances that no longer justify this decision, the Commission may amend, suspend, or repeal the decision, or negotiate with the third country to remedy the issues identified.[312]

Further, under the GDPR, national data protection authorities ("DPAs") are empowered to ban cross-border data flows and limit data exports, whether to prevent harm or to bring the transfers into conformity with EU standards.[313] This corrective power can be applied to all data exports, including those relying on an adequacy finding, "appropriate safeguards", and "derogations". In particular, national DPAs have the competence to examine data transfers to a third country that has obtained an "adequate decision" from the Commission.[314] As such, the data embargo power under EU data protection law is prominent and pervasive, capable of monitoring and sanctioning recalcitrant third countries and their digital firms for breaching European data subjects' fundamental rights.

Third, the institutional design of EU's fundamental rights paradigm would lock in an important dynamic oriented at securing sufficient data protection as a normative priority. To start with, under the GDPR, it is the EDPB that advises on the Commission on the making of an "adequacy" decision over a third country's data governance system for the purpose of TPDF.[315] The EDPB, a new institution under the regulation, is an independent, consultative body composed of representatives of national DPAs and the European Data Protection Supervisor (the EU's independent DPA).[316] This creates an institutional framework for national and EU DPAs to

---

[310] See *infra*, Part II(A) and (B).

[311] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. R. 1966, 1966, 1984 (2013).

[312] COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (GDPR) BY EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS 255 (2018).

[313] GDPR, art. 58(2). See Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 Iowa L. R. 471, 488-489 (1995) (categorizing DPAs' "data embargo order" into "a preventative data embargo order" (aimed at preventing harm) and "a structural order" (that "restructures or otherwise alters a planned data transfer to bring it into conformity with" applicable EU data protection law)).

[314] GDPR, art. 58(2); C-362/14, *Maximilian Schrems v. Data Protection Commissioner* [GC], October 6, 2015, ECLI:EU:C:2015:650, paras. 63, 65–66.

[315] Official Website of the European Data Protection Board: Who We Are, https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en.

[316] *Id.* See ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 94 (2008) ("Under the EU Directive 1995…. (a) standing committee of national data privacy authorities, the Article 29 Working Party, was created to advise the European Commission… to evaluate the adequacy of privacy protection in non-EU countries.")

develop a consensus on transnational data privacy issues and to evaluate the adequacy of a third country's protection.

Conceptually, the EDPB could be understood as a transnational regulatory network (or an "epistemic community") engaging in data privacy policymaking and embedded into the EU's governance institutions.[317] Notably, its constituents—national and EU's DPAs—are a group of highly networked "knowledge elite" with recognized competence and expertise in data privacy protection.[318] Sharing common normative commitments to protecting data privacy, these actors are equipped with the power resources of expertise, delegated political authority, network ties, and professional prestige in data privacy protection, which is an issue-area highly valued by key political actors and the society at large.[319] Relying on their regulatory expertise and capacity, the EU institutions (such as the Commission) and member state political actors delegate important policymaking authority to them on data privacy protection. Thus, when evaluating the "adequacy" of a foreign jurisdiction, the EDPB would be primarily concerned with whether and how fundamental rights of EU citizens could be adequately protected as a policy priority, rather than how international trade could be facilitated.

Further, in terms of law enforcement and judicial review, the authority to examine and review whether cross-border data flows to a third country comply with EU data protection standards largely belong to national DPAs and European judiciary (the ECJ and national courts). This institutional design delegates investigative and decision-making authority to a plurality of independent supervisory agencies and judicial trustees at multiple levels, which commonly perceive their primary responsibilities as safeguarding Europeans' fundamental rights.[320] Driven by their shared normative commitments, these institutional actors can manifest "a continuous dynamic of mutual reinforcement", and their mutual influences may enhance the overall human rights standards on a transnational level. In that regard, a notable instance is the *Schrems II* case.

In July 2020, the ECJ invalidated the EU-U.S. Privacy Shield agreement—a transatlantic commercial data exchange instrument which the Commission considered as providing an "adequate" level of data protection.[321] The Court found that due to disproportionate U.S. surveillance practices, U.S. public authorities could access and use personal data transferred from the EU in ways violative of the fundamental rights of EU citizens, who had no effective legal remedy to protect their rights against potential abuses.[322] With respect to data transfers via the

[317] See Newman, *Building Transnational Civil Liberties—Transgovernmental Entrepreneurs and the European Data Privacy Directive*, 62 INT'L ORGAN. 103 (2008) (discussing the role of transgovernmental actors (EU member states' DPAs) as "policy entrepreneurs within (EU's) multilevel structure", which was crucial to the draft and passage of the DPD).

[318] Peter M. Haas, *Introduction: Epistemic Communities and International Policy Coordination*, 46 INT'L ORG. 1, 3 (1992).

[319] *Id.*, 4, 7, 17; Newman, *supra* note (*Building Transnational Civil Liberties*), 120.

[320] Henry Farrell & Abraham Newman, *Schrems II Offers An Opportunity—If the US Wants to Take It*, LAWFARE (July 28, 2020), https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it ("American proposals to respond to *Schrems II* by punishing the European Union through trade sanctions or the like will fail, because they don't affect the relevant decision makers. Like the U.S. Supreme Court, the CJEU has its own politics but it does not negotiate. Instead, it lays down authoritative interpretations of the law … (and national DPAs) see their fundamental responsibility as protecting the rights of EU citizens, rather than facilitating international trade.")

[321] Schrems II, para. 201.

[322] *Id*., para. 179-199.

SCCs, the ECJ held that, competent national DPAs must suspend or prohibit cross-border personal data transfers to a third country, if they were of the view that the SCCs were not or could not be fulfilled in that country, and no other means can ensure the required level of protection for the transferred data.[323] While the Court suggested that it was possible to use "supplementary measures" to adequately protect data under the SCCs, it did not specify what those measures can be.[324]

The implications of this decision are three-fold. First, the Court's "fundamental rights-inspired interpretations" forced the Commission to renegotiate transatlantic personal data transfer agreements with stronger data protection standards against foreign governments' surveillance practices.[325] Within the EU's institutional structure, it is the Commission that is responsible for negotiating international treaties on behalf of the EU.[326] When negotiating the Safe Harbor agreement, the Commission seemed to have treated commercial data transfers as separate and distinct from national security issues, out of the pragmatic considerations to strike a deal to enable transatlantic TPDF. However, the ECJ clearly disagreed, and found the relatively weak administrative procedure of the Safe Harbor insufficient to safeguard Europeans' fundamental rights, particularly in light of the Snowden revelations.[327]

This means that while the Commission can make strategic trade-offs to facilitate TPDF out of economic considerations, the Court would impose a boundary to delineate what is off-limit, serving as a constitutional "gatekeeper" that prioritizes adequate protection of fundamental rights. At a deeper level, this European constitutional check-and-balance mechanism makes it particularly difficult for the Commission to water down the adequate level of data protection through international negotiations.[328]

More generally, this ruling also requires the Commission to exercise greater scrutiny over a foreign jurisdiction's surveillance laws and practices when determining whether to issue or maintain an adequacy decision. In the face of this ruling, it is conceivable that this enhanced scrutiny of review would be exercised over countries that hope to obtain new adequacy decisions from the Commission. Even for jurisdictions that have achieved an adequacy status, this judicial decision also may pressure them to satisfy the Commission that their domestic data privacy protections against intelligence surveillance are robust and justiciable—otherwise, the Commission could alter, amend, or withdraw those decisions.[329]

---

[323] *Id.*, Ruling, para. 3.

[324] *Id.*, para. 133. See Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUROPEAN LAW BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.

[325] Ryngaert & Taylor, *supra* note, 7.

[326] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 9 (2020).

[327] Farrell & Newman, *supra* note (*Schrems II*) ("The Snowden leaks allowed Schrems to persuade European judges that one couldn't regulate the (commercial data exchange) without addressing (national security issues), closing off the space for possible compromise.").

[328] Yakovleva, *supra* note (Privacy Protectionism), 466 (noting that the rights to privacy and the protection of personal data are fundamental rights enshrined in the EU Charter of Fundamental Rights, a constitutional instrument with the highest legal force in EU law). The ECJ is the court of last resort with the final say on the interpretation and application of the EU Charter.

[329] Chander, *supra* note, at 775 (noting that the Commission has been reviewing the adequacy decisions (with Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay) since 2017).

Second, through its authoritative interpretations of the EU law, the Court exerted pressure on foreign governments and private firms that desire unrestricted personal data flows from Europe to enhance protection for EU data subjects' personal data.[330] Though not spelling out what kinds and levels of additional safeguards would be "adequate", the ECJ shifts the burden to these private and public actors, incentivizing them to ensure compliance with EU standards under the shadow of pervasive data embargo power. In particular, this substantially complicates data exports from the EU through the SCCs, potentially turning them into "mini adequacy decisions" in effect.[331]

Third, as noted earlier, the Court empowered national DPAs to investigate and block SCC-based data transfers to the U.S., if they considered that U.S. surveillance programs would inevitably enable the U.S. government to access EU citizens' data in breach of European data protection standards. In the aftermath of this case, Portugal's DPA sought to block certain data exports via the SCCs to the U.S.,[332] and Germany's Berlin DPA likewise called for EU-based data controllers exporting data to the U.S. to transfer those data to the EU.[333] In these two instances, the Portuguese and Berlin DPAs questioned the legality of outbound data transfers through the SCCs, based on the perceived high risks imposed by U.S. intelligence surveillance to EU data subjects' fundamental rights. Indeed, not all national DPAs may take the same approach. Yet, by establishing authoritative interpretations of EU law at the top layer of the EU's multilevel governance system, the ECJ creates an institutional incentive for various like-minded national DPAs to follow suit, thereby fostering "an expansion of the norms and institutions for the protection of fundamental rights in other layers."[334]

C. A National Security Paradigm to Regulate TPDF

---

[330] Ryngaert & Taylor, *supra* note, 7.

[331] Kuner, *supra* note (Schrems II) ("(Under the judgment) … Data controllers will be expected to conduct a detailed examination of the circumstances surrounding each transfer, the adequacy of protection in the country to which the data will be transferred, and the parties processing the data. The fact that the Court expects data controllers to verify that there is an adequate level of protection in the country of import, a role that Art. 45 GDPR reserves to the Commission, would seem to make use of the SCCs in effect "mini adequacy decisions".).

[332] *Portuguese DPA Orders Suspension of U.S. Data Transfers by Agency That Relied on SCCs*, HUNTON ANDREWS KURTH (April 28), 2021, https://www.huntonprivacyblog.com/2021/04/28/portuguese-dpa-orders-suspension-of-u-s-data-transfers-by-agency-that-relied-on-sccs/ ("On April 27, 2021, the Portuguese Data Protection Authority (... the "CNPD") ordered the National Institute of Statistics (the "INE") to suspend, within 12 hours, any international transfers of personal data to the U.S. or other third countries that have not been recognized as providing an adequate level of data protection… Upon receiving a number of complaints, the CNPD started an investigation into the INE's data transfers outside of the EU. The CNPD concluded that Cloudfare is directly subject to U.S. surveillance laws for national security purposes. According to the CNPD, those surveillance laws impose a legal obligation on companies like Cloudfare to give unrestricted access to personal data to U.S. public authorities without informing data subjects.").

[333] *Berlin: Berlin Commissioner Issues Statement on Schrems II Case, Asks Controllers to Stop Data Transfers to the US*, ONE TRUST DATA GUIDANCE (July 17, 2020), https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data ("the Berlin Commission called for data controllers based in Berlin storing personal data in the US to transfer the same to Europe… (with respect to the SCCs, it) highlighted that, pursuant to the judgment, European data exporters and data importers in third countries are obliged to check before the first data transfer whether the third country has state access to the data that goes beyond what is permitted under European law and that, if such access rights exist, SCCs cannot justify the data transfer to such third country."). https://www.skadden.com/insights/publications/2020/07/privacy-cybersecurity-update.

[334] FABBRINI, *supra* note, 13-14.

Unlike the economic and the rights-oriented framings, the security-based conceptualization of personal data justifies a national security paradigm. Underpinned by an increasingly expansive conceptualization of national security interests, China deploys a comprehensive set of domestic security institutions to regulate TPDF. Focused on the national security implications of personal data, this approach seeks to localize data storage within a state's territory, subject to limited exceptions of cross-border data flows.

(A) The Underlying National Security Logic

In Section II.C, this chapter discussed China's security-oriented conceptualization of personal data, focused on how personal data could affect national security (through "data security" and "economic security").[335] Conceptualizing personal data through the national security prism requires a distinct basic logic, generating far-reaching policy implications for the institutional design to regulate TPDF.

First, while its historical narrative has long focused on typical military defence (against armed attack and territorial invasion), the meaning of "national security" has evolved over time to become increasingly expansive, particularly given the transformative effects of data-driven technologies and the U.S.-China geopolitical rivalry.[336] In the digital era, an adversary could utilize AI-powered technologies to destabilize and degrade a target state, without resorting to an armed conflict. As a result, the notion of national security has expanded far beyond the narrow scope of "military preparedness", and now includes "a wide range of important bulwarks in defense of the good of the nation such as protection from political instability, avoiding technological degradation, retaining economic stability and securing vital supply-chains."[337]

Under this new conceptualization, protecting "national security" means that a state must keep its existence and legitimacy, its property, and its citizens safe from various security threats—whether external or internal, physical or virtual, political, economic, or military.[338] This dynamic concept thus requires the government to leverage various power levers—including political power, economic power, military might, and foreign policy tools—to achieve its security goals.

In particular, defending a sovereign's property (beyond physical borders and territorial integrity) entails protecting important industries, fundamental infrastructures, national champions, critical technologies, as well as sensitive and important data,[339] whose vulnerability could significantly undermine a nation's overall security. This entails a "geo-economic" logic: a sovereign government could use economic instruments and policies to defend and promote national security interests (far beyond the narrow economic goals in the market's terms) as a lever of national power.[340]

---

[335] See *infra* Section II.C.
[336] Joel Slawotsky, *The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualization*, 20 CHINESE J. INT'L L. 3, 61-62 (2021).
[337] *Id.*
[338] *Id.*, 53. See Chaisse, *supra* note (*Demystifying*), 596.
[339] Slawotsky, *supra* note, 53-54.
[340] Jane Golley et al., *Geoeconomics and the Australian University Sector: A "Geoeducation" Analysis*, 16 SECURITY CHALLENGES 24, 24-25 (2020).

Second, national security is largely an important "public good" that individuals, firms, or the markets cannot readily provide. Relying on the latter could put national security at risk, since these actors and mechanisms have neither the incentives nor the capacities to supply this public good—at least not to a sufficient level. Instead, a society must depend on the state and its public power to secure cybersecurity and national security.[341] As put by President Xi, to adequately safeguard cybersecurity, "there must be *unified planning, unified deployment, unified promotion, and unified implementation*" by the state from the top level of national policy-making.[342]

By implication, neither the economic paradigm nor the fundamental rights paradigm is suitable to provide a satisfactory institutional framework to safeguard and advance national security interests. This is particularly true in case of TPDF regulation. Driven by an overarching normative goal of economic efficiency, the trade paradigm pursues unrestricted personal data flows to maximize economic welfare and technological advancement. However, this paradigm makes national security regulations an exception *a priori* in need of justification under a strict, objective "necessity" test.

Typically crafted with a "rules-exceptions" structure, international trade and investment agreements may prove capable in handling extreme cases of thinly veiled, blatant protectionism under the disguise of "national security". But this institutional suitability no longer holds, to the extent it is difficult to distinguish pretextual and abusive measures from good-faith regulations driven by legitimate national security concerns in response to novel challenges (such as cyber-crimes, threats to infrastructures, industries, and the media, and transnational terrorism, etc.).[343]

In such less clear-cut scenarios, it is quite challenging for international adjudicators mandated by international economic agreements to step into difficult, controversial, and unresolved issues of national security, and to balance trade or investment interests with sensitive domestic political, social, and cultural values. Further, it is questionable whether international economic lawyers have the expertise, competence, and legitimacy to scrutinize value-laden, polycentric internal political and regulatory decision-making, to address the uncertainties pervading digital technologies, and to cross the boundary of international legal regimes.[344] To make things more complicated, many of these policy questions are of a *political* nature, and different societies may have distinct values and preferences. As a result, acute legitimacy problems arise as to whether international economic agreements and their dispute resolution mechanisms are a *suitable* institution to strike a proper balance between international trade and national security interests underlying TPDF, particularly on a routine basis.

---

[341] Yanqing Hong, *The Cross Border Data Flows (Data Exit) Security Assessment: An Important Part of Protecting China's Basic Strategic Resources*, RESEARCH ALLIANCE FOR DATA GOVERNANCE AND CYBER SECURITY (January 4, 2018), http://www.dgcs-research.net/a/Opinion/2018/0103/59.html.

[342] *Id* (emphasis added).

[343] Benton Health, *National Security and Economic Globalization: Toward Collision or Reconciliation?*, 42 FORDHAM INT'L L. J. 1431, 1432 (2019); Benton Health, *The New National Security Challenge to the Economic Order*, 129 YALE J. INT'L L. 1020, 1020 (2020). See Julian Arato et al., *The Perils of Pandemic Exceptionalism*, 114 AM J. INT'L L. 627 (2020).

[344] Arato et al., *supra* note, 6; Heath, *supra* note, 1432; Neha Mishra, *The Trade—(Cyber)Security Dilemma and its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567, 571-572 (2020).

In short, as regards the trade paradigm, its economic-oriented normative priorities and rule-exception structure cannot adequately safeguard national security interests implicated by personal data. The same also goes for the fundamental rights paradigm, whose normative focus is to protect individuals' human rights and civil liberties, rather than a country's national security.

Third, addressing national security interests on a regular basis requires a security-oriented paradigm to govern sensitive economic activities. Under this paradigm, restrictions on free trade and civil liberties for the interests of national security become non-negotiable.[345] And the default rules to regulate TPDF should ensure national security as a matter of priority. In the extreme, the government may make outbound data transfers an exception that is allowed on an *ad hoc* basis, and which is based on a security-oriented review process. Consequently, the decision-making authority should be delegated to security-minded institutions at the national, rather than international, level.

Indeed, many commentators may be concerned that in international economic law, unfettered broadening of the national security exceptions could increasingly engulf the rules themselves.[346] Yet, with respect to TPDF, such tensions suggest that this issue-area is increasingly caught between two different models of governance—the economic paradigm and the national security paradigm. In this sense, the exception clauses in international trade agreements become an invisible door linking these two parallel universes.[347] With different normative benchmarks, policy priorities, default rules, and exceptions, these paradigms increasingly compete to regulate TPDF, striving to reposition its governance within their own jurisdictions and domains.

(B) An Institutional Framework Oriented at Safeguarding National Security

To fully understand China's security-oriented paradigm to regulate TPDF, it is worth noting an overarching institutional framework that the former is embedded in. At a foundational level, China's National Security Law 2015 has established a national legal and regulatory framework to safeguard national security interests against various domestic and external threat actors.[348] Within this institutional structure, the Cybersecurity Law, Personal Information Protection Law, Data Security Law, as well as associated administrative regulations were subsequently enacted to regulate more specific issues of cybersecurity, data security, and cross-border data transfers.

1. National Security Law 2015

From the outset, China adopted the first National Security Law in 1993, which aimed to "legalize national security affairs" and offer a "legal weapon" to safeguard national security.[349] Yet, the "national security" threats dealt with by that law were limited to "external" interference originating

---

[345] Martina F. Ferracane & Hosuk Lee-Makiyama, *China's Technology Protectionism and Its Non-Negotiable Rationales*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (June 2017), at 15, https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf.
[346] See e.g., Slawotsky, *supra* note, 3-4.
[347] Cohen, *supra* note, 802.
[348] National People's Congress, National Security Law, promulgated in July 2015, arts. 1-3, http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm ["National Security Law 2015"]
[349] Congyan Cai, *Enforcing a New National Security? China's National Security Law and International Law*, 10 J. E. ASIA & INT'L L. 65, 78 (2017).

from foreign-related actors (private or public),[350] with a focus on espionage and intelligence gathering.[351] Not surprisingly, this law became increasingly outdated and insufficient to address novel national security threats, which extend beyond the narrow context of military attack and foreign espionage.[352]

In this context, a new National Security Law was enacted in 2015, which reconceptualized "national security" and revamped the national security regime. Under this new law, "national security" is broadly defined as "a situation where the national political regime, sovereignty, national unity and territory integrity, people's welfare, sustainable development of the economy and society, and other fundamental national interests are immune from dangers and external and internal threats".[353] Meanwhile, the notion of "national security" also covers the capability to continuously maintain and preserve these security interests.[354] Further, the law incorporates a holistic conceptualization of national security, originally raised by President Xi Jinping in 2012.[355] That is, national security must treat political security as the core, regard economic security as the foundation, and have military, cultural, and social security as safeguards, while enhancing a country's international security.[356]

As such, the reconceptualized notion of national security is broad, expansive, and somehow vague. For our purpose, it bears noting that China's dominant conceptualization of national security has developed into a fused mass of interests, composed of three major pillars—political security and societal stability, economic security, as well as technological interests.

Regarding economic security, the National Security Law emphasizes the necessity of ensuring the security of key industries and economic sectors, critical infrastructures, and other important economic interests.[357] With respect to technological interests, the law stresses the importance of relying on self-driven innovation capacities to develop cutting-edge technologies and critical technologies in key areas. [358] While these terms seem ambiguous and imprecise, telecommunication infrastructures (such as 5G) and data-driven technologies (AI, robotics, cloud computing) obviously fall into their ambit. As such, maintaining economic competitiveness and safeguarding vital supply-chains in these industries and sectors are framed as China's legitimate national security interests.

Further, the National Security Law treats cybersecurity as a matter of national security. Specifically, the law requires the state to enhance cybersecurity capacities, and to make core informational technologies, critical infrastructures, and *data "secured and controllable"*, in order to achieve cyber sovereignty and development interests.[359]

---

[350] Hualin Fu & Richard Cullen, *National Security Law in China,* 34 COLUM. J. TRANSNAT'L L. 453 (1996).
[351] Cai, *supra* note, 78-79.
[352] *Id.*, 79, 80 (noting that "most of provisions of (this law) were merged into the Law of Espionage 2014.").
[353] National Security Law 2015, art. 2. Cai, *supra* note, 80.
[354] National Security Law 2015, art. 2.
[355] Cai, *supra* note, 81.
[356] National Security Law 2015, art. 3.
[357] *Id.*, art. 19.
[358] *Id.*, art. 24.
[359] *Id.*, art. 25 (emphasis added).

At the implementation level, the National Security Law mandates the Chinese government to establish the national security review mechanisms, covering foreign investment screening, export control of certain goods and critical technologies, and cybersecurity review of network information products and services.[360] Given that the law applies a "*precautionary principle*" to address both actual and potential threats to national security,[361] active enforcement of the National Security Law could subject wide-ranging economic areas to the review processes, as long as the underlying activities impact or are likely to impact national security. And for these national security review mechanisms, no meaningful rule-of-law institutions exist to effectively check and balance the government's exercise of public power.[362]

2. Cybersecurity Law 2016

To implement the mandates of the National Security Law 2015, a series of subsequent legislations were promulgated to regulate cybersecurity and data security. In 2016, China enacted the Cybersecurity Law, the first comprehensive national legislation devoted to cybersecurity. In its first article, this law recognizes cybersecurity as an important pillar of national security and cyber sovereignty.[363]

Although mainly focused on cybersecurity and cyber sovereignty, this law stipulated a comprehensive set of personal data protection rules.[364] Unlike prior data privacy regulations that were largely sectoral, this law is a comprehensive legislation, broadly applying to all network operators across various sectors.[365] Yet, different from the European notion of fundamental rights, the Cybersecurity Law frames personal data protection as a key pillar of "data security" (or "network information security"), undergirding a country's cybersecurity.[366] In addition to substantive provisions on "network information security" and "personal information protection", this law also establishes the default rules of "data localization" to govern cross-border data transfers.[367]

Prior to the enactment of the Cybersecurity Law, the applicable rules governing cross-border data flows were scattered across numerous sectoral laws and regulations, which addressed specific industries or select categories of data, such as personal financial data, credit information, human genetic data, demographic health data, geolocation data, and map data.[368] Though generally requiring localized storage and processing of data, these rules were of a sectoral nature, and their implementation typically remained weak in practice, such that much of cross-border data flows

[360] *Id.*, art. 59.
[361] Cai, *supra* note, 81; see e.g., *Id.*, art. 3.
[362] Cai, *supra* note, 79.
[363] Cybersecurity Law 2016, art. 1.
[364] Keming Cai, *Jurisdictional Report: People's Republic of China*, in REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 63 (Clarisse Girot ed., 2018), https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/# ["*Jurisdictional Report*"].
[365] *Id*., 64. See Cybersecurity Law 2016, arts. 21-50.
[366] Entitled "Network Information Security", chapter 4 of the Cybersecurity Law contains provisions on protection of personal information and online content regulation (i.e., arts. 40-50). See Cai, *Jurisdictional Report*, 63-64; Hong, *supra* note; Cybersecurity Law, arts. 40-50.
[367] Hong, *supra* note. See *infra* Section III.C(C).
[368] Cai, *supra* note (*Jurisdictional Report*), 65-72.

from China went largely unregulated.[369] This status quo was dramatically changed by the Cybersecurity Law, which is the first national legislation that explicitly stipulates data localization requirements across all sectors.

In that regard, article 37 of this law requires critical information infrastructure ("CII") operators to store personal data and important data that they collected and processed in China within its territory.[370] Outbound data transfers are only permitted if they are necessary due to CII operators' business purposes, and must pass the security assessments organized by the Cyberspace Administration of China (CAC) and other regulatory authorities within the State Council.[371]

By definition, CII refers to important network infrastructures and information systems that would seriously harm national security, economic security, or public interests, if they were impaired, dysfunctional, or suffered data breaches.[372] According to the CAC (a leading Chinese authority to regulate the Internet),[373] CII could be grouped into three categories: websites (e.g., news media, websites of the government, public institutions, and enterprises), Internet platforms (such as social media, e-commerce, e-payment, search engines, and other Internet service providers), as well as production operations (including office and business systems, industrial control systems, big data centers, cloud computing, television and broadcast systems).[374] Such a broad definition with an imprecise boundary could cover major information technology suppliers and digital service providers that reach a certain scale, as long as regulatory authorities perceive significant risks to security interests at the national and societal levels.

Under a risk-based approach, "important data" is defined as "data that, if leaked, may directly affect China's national security, economic operations, social stability, or public health and safety".[375] The determination of "important data" depends on what interests the data could impact, rather than who controls those data: personal data held by a private firm could qualify as such, as long as it may endanger national security and public interests.[376]

---

[369] *Id*. 72. An exception is "state secrets", as broadly defined as "any non-public information or matter that has a vital bearing on state security and national interests". Transfers of state secrets out of China is not only completely prohibited, but also more vigorously enforced. Id., 66-67, 73.
[370] Cybersecurity Law 2016, art. 37.
[371] *Id.*
[372] *Id.*, art. 31.
[373] See *infra* section III.C.(C).
[374] State Council, Provisions on the Safety and Protection of Critical Information Infrastructure Security, July 30, 2021, art. 2, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm (The determination of the list of CII should be made by relevant supervisory governmental authorities, taking into account of these factors: the importance of the network facilities and information systems to the core business of the industry and sector, the harm caused in case of attack or breach, and impact to other industries and sectors). *Id.*, art. 31 (examples of CII include "telecommunication, information services, energy, transportation, water facilities, finance, e-governance, public services, national defence technologies.").
[375] Cyberspace Administration of China, *Measures on Security Assessments for Cross-Border Data Transfers*, issued on July 7, 2022, effective on September 1, 2022, art. 19, https://www.lawinfochina.com/display.aspx?id=39000&lib=law [Security Assessment Measures].
[376] Hong, *supra* note ("determining what constitutes 'important data' requires us to stop judging by who holds the data and instead proceed by determining what values and interests the data can affect.").

3. Personal Information Protection Law 2021

After the Cybersecurity Law, Chinese authorities continued to push for a more comprehensive legal framework through domestic legislative process to regulate the data-driven business models and practices of Chinese tech giants and online platforms.[377] To strengthen regulatory control over data processing and safeguard national data security, China adopted the Personal Information Protection Law in August 2021.[378]

In addition to establishing a comprehensive legal framework to protect personal data against data controllers,[379] this legislation stipulates more expansive data localization requirements. On top of the Cybersecurity Law's mandate (i.e., article 37), the Personal Information Protection Law further requires data controllers whose data processing activities reach the CAC's stipulated volume thresholds to locally store personal data that they collected and generated in China.[380]

As clarified by a subsequent CAC regulation, such thresholds would be triggered, if a data controller (i) has processed personal data of over 1 million people, or (ii) has cumulatively exported personal data of more than 100,000 people or sensitive personal data of more than 10,000 people since January 1 of the previous year.[381] For data controllers falling into this scope, they must store personal data within China's territory by default.[382] As with CII operations, for these controllers, transfers of personal data outside China are only possible when necessary for their business requirements, and must pass the scrutiny of the security assessments organized by the CAC.[383]

In the security assessments, the CAC adopts a holistic approach to comprehensively evaluate the security risks imposed by the proposed data transfers, with a focus on the threats for national security and public interests.[384] The particulars to be reviewed in the assessment process generally include (i) the legality, propriety, and necessity of the data transfers, (ii) the volume, scope, type, sensitivity, and potential risks of the underlying data, (iii) the impact of the recipient jurisdiction's data protection laws, regulations, and policies on the security of the data to be transferred, (iv) whether a recipient party's data protection obligations assumed under the contract and its data protection measures and capacities are sufficient, and (v) the security risks generated during and after the data transfers (such as the disclosure, breach, damage, and misuse of, or unauthorized access to those data).[385] While the specific standards applied to scrutinize data transfers are unclear, the security-minded CAC is very likely to decline the application, where it considers that the transfers may infringe on China's national security interests.

---

[377] Rogier Creemers, *China's Emerging Data Protection Framework*, 8 JOURNAL OF CYBERSECURITY 1, 5-6 (2022). See *infra* chapter 5 ("China's Data Sovereignty"), section III.B.(B).
[378] National People's Congress, *Personal Information Protection Law of the People's Republic of China*, promulgated in August 2021, http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml ["Personal Information Protection Law 2021"].
[379] See *infra* chapter 5 ("China's Data Sovereignty"), section III.B.(B).
[380] Personal Information Protection Law 2021, art. 40.
[381] Security Assessment Measures, art. 4.
[382] Personal Information Protection Law 2021, art. 40.
[383] *Id.*
[384] See Security Assessment Measures, *supra*, art. 8.
[385] *Id.*, arts. 5, 8. For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.A.(A).

For controllers whose data processing has not triggered the CAC's thresholds, the Personal Information Protection Law provides for two parallel mechanisms of cross-border data transfers, in addition to the security assessment process.[386] The first is the certification mechanism, requiring a data controller to apply for certification from an accredited agency pursuant to the CAC's requirements.[387] Designed to implement uniform data protection rules for data processing activities within multinational organizations, the certification mechanism requires a data controller and a recipient (such as affiliated companies of a corporate group) to conclude binding and enforceable legal instruments to ensure a data protection level that is equivalent with that under the Chinese law.[388] Second, data controllers may also rely on a standard contractual agreement formulated by the CAC to transfer personal data outside China.[389]

While opening an alternative avenue for outbound data transfers, the certification mechanism and standard contractual agreements are subject to their own limits and restraints. Due to the volume thresholds that would trigger a mandatory security assessment, these two mechanisms of data exports cannot offer a long-term solution for data-intensive companies' large-scale transfers of personal data. Further, these two mechanisms are relatively inflexible and costly,[390] generating considerable compliance costs and administrative burdens for data exporters.

Finally, the Personal Information Protection Law imposes additional compliance requirements for each mechanism of cross-border data transfers, ranging from security assessments to certification to standard contractual agreements. As a precondition for exporting personal data abroad, a data controller must inform a data subject of the specifics about the data transfer, and obtain the latter's informed consent.[391] Meanwhile, before transferring data abroad, data controllers also need to conduct data protection impact assessments to evaluate the legality, propriety, and necessity of the data transfers, the security risks imposed to data subjects, and whether the protective measures are legal, valid, and proportionate.[392]

4. Data Security Law 2021

---

[386] Personal Information Protection Law 2021, art. 38(1)(a)-(c).
[387] *Id*., art. 38(1)(b).
[388] TC260, *Technical Specification on Certifications for Personal Data Cross-Border Processing Activities*, December 2022, arts. 2, 5, https://www.tc260.org.cn/front/postDetail.html?id=20221216161852 [Certification Specification]. For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.A.(B).
[389] *Id.*, art. 38(1)(c). See CAC, *Provisions on Standard Contractual Agreements for Outbound Transfers of Personal Data*, promulgated on February 22, 2023, effective on June 1, 2023, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm. For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.A.(B).
[390] For instance, to comply with the certification requirements, both the data controllers and recipients must designate their data protection officers and establish their data protection departments, respectively, making this mechanism relatively costly for firms exporting small amounts of personal data. And to use the CAC-formulated model contract, the data controllers must complete the mandatory filing procedure with the CAC (to file the contractual agreements and data protection impact assessment reports in record), potentially generating high administrative burdens for data-reliant firms that often demand routine, regular, and continuous data flows. For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.A.(C).
[391] Personal Information Protection Law 2021, art. 39.
[392] *Id.*, art. 56.

Another pillar to safeguard cybersecurity is the Data Security Law, which was enacted in June 2021.[393] This law seeks to set forth a regulatory framework to protect the broadly defined "data security" in China, with a focus on "important data".[394] Specifically, this legislation mandates the establishment of several important mechanisms to safeguard national security interests underlying "important data".

First, the law mandates the government to establish a "categorical and hierarchical system" to protect data security.[395] Under this system, the degree of protection afforded will vary, based on the relative importance of the data in economic and social development, as well as the degree of damage generated to national security and public interests once such data is breached, disclosed or misused.[396] At the top of the hierarchy is "national core data" (i.e., the data that is most closely related to national security, the national economy's lifeline, and exceptional public interests), which must be subject to more stringent regulatory control.[397] To enhance national data security, the government should make lists to catalog "important data" and "national core data", and establish a centralized mechanism to assess, analyze, monitor, and control potential data security risks.[398]

Second, the government is mandated to establish the data security review mechanism, which is designed to scrutinize data processing activities that impact or are likely to impact national security.[399] The decisions made out of this review process are binding and final.[400]

A notable example in that regard is the Didi's case, where the CAC has deployed the national security review process to scrutinize potential cross-border data transfers. In that case, following the U.S. listing of Didi Chuxing (a Chinese ride-hailing digital platform), the CAC launched an investigation on Didi on the grounds of data security and national security,[401] marking the first cybersecurity review over a Chinese tech giant.[402] Allegedly out of the concerns that Didi may have to provide sensitive personal data to U.S. authorities, the CAC ordered various Chinese app stores to remove Didi from their platforms, and requested Didi to postpone its U.S. listing until potential national security threats were cleared.[403]

---

[393] Data Security Law 2021, *supra* note.
[394] Yan Luo & Zhijing Yu, *China Issued the Draft Data Security Law*, COVINGTON UPDATES ON DEVELOPMENTS IN DATA PRIVACY AND CYBERSECURITY (July 3, 2020), http://www.insideprivacy.com/data-security/china-issued-the-draft- data-security-law/.
[395] Data Security Law 2021, art. 21.
[396] *Id*.
[397] *Id*.
[398] *Id.*, arts. 21-22.
[399] *Id.*, art. 24.
[400] *Id.*
[401] Zhijing Yu, Vicky Liu & Yan Luo, *China Initiates Cybersecurity Review of Didi ChuXing and Three Other Chinese Mobile Applications*, COVINGTON: INSIDE PRIVACY (July 6, 2021), https://www.insideprivacy.com/international/china/china-initiates-cybersecurity-review-of-didi-chuxing-and-three-other-chinese-mobile-applications/ (According to the announcements of the Cybersecurity Review Office (an authority established within the CAC), this cybersecurity review was "initiated based on requirements under the *National Security Law* … the *Cybersecurity Law* … and the *Measures on Cybersecurity Review* … and are aimed at 'preventing national data security risks, maintaining national security and safeguarding public interests.'").
[402] Jane Li, *China's Big Tech Crackdown Has Opened A New Front: National Security*, QUARTZ (July 12, 2021), https://qz.com/2031886/chinas-big-tech-crackdown-is-now-targeting-national-security/.
[403] *Id*.

While many Chinese firms have listed in the U.S., in the eyes of the CAC, the situation is very different for Didi. As a dominant player that has taken over eighty percent of China's ride-hailing market, Didi effectively controls the largest trove of personal travel data in China.[404] As to the cybersecurity review of Didi, the point is not whether personal data held by a foreign-based private firm is typically shared with the U.S. government as part of the U.S. securities listing processes. Rather, the CAC's major concerns seem to stem from the fact that Didi has subjected itself to the jurisdiction of U.S. authorities by listing in a U.S. stock exchange. This makes it possible for the U.S. government to force a Chinese tech giant holding a myriad of sensitive personal data to handle over such data—whether publicly or clandestinely, in the course of the listing or afterwards, under the CLOUD Act, U.S. securities regulations, or U.S. intelligence surveillance programs.[405] Under a security mindset, such a future-oriented possibility could translate into a systemic vulnerability, undermining China's national security interests.[406]

Finally, the Data Security Law mandates the government to implement export control over data that belongs to controlled items and which is related to protecting national security and national interests (or fulfilling international obligations).[407] While ambiguities surround this provision, commentators tend to construe it as imposing a stricter condition on the export of certain "important data".[408] This means that such data transfers must undergo the scrutiny of China's Export Control Law, which deploys a comprehensive framework to ban and restrict the export of military and dual-use products, technologies, and services bearing national security interests.[409]

(C) The Cyberspace Administration of China as a Centralized Regulatory Authority

Throughout several rounds of revamp, China's Internet regulation has evolved all the way "from the regulation of the hardware and then software, to the regulation of content and now data."[410] In

---

[404] See an op-ed by Global Times (China's state-owned media outlet): *Why Didi's Removal from App Win Public Support: Global Times Editorial*, GLOBAL TIMES (July 5, 2021), https://www.globaltimes.cn/page/202107/1227859.shtml

[405] Li Qiaoyi & Zhang Hongpei, *3 More Internet Firms Scrutinized Amid Rising Data Security Concern*, GLOBAL TIMES (June 5, 2021), https://www.globaltimes.cn/page/202107/1227899.shtml ("The hypothetical scenario of the US coercing Chinese firms to submit data could happen, experts said, citing the US government's track record of stopping at nothing to forcing businesses to surrender … Foreign Minister spokesperson Wang Wenbin said that time and again, it has been demonstrated that it is the US that forces companies to open "back doors" and illegally obtain user data.").

[406] *Id.* ("No internet giant is allowed to become a super database that has more personal data about the Chinese people than the country does, not to mention using the data at its own will… For companies like Didi which have gotten listed in the US market and whose largest and second largest shareholders are foreign companies, China should more strictly supervise their information security to protect both personal data security and national security.").

[407] Data Security Law 2021, art. 25.

[408] See eg., Xuan Wu, *The Construction of Personal Information Cross-Border Transfers Rules under A Digital Sovereign Perspective*, 15 TSINGHUA LAW REVIEW 74, 83 (2021) [吴玄，《数据主权视野下个人信息跨境规则的建构》，《清华法学》2021 年第 15 期].

[409] Nathan Bush et al., *China's New Export Control Law*, DLA PIPER PUBLICATIONS (October 19, 2020), https://www.dlapiper.com/en/us/insights/publications/2020/10/chinas-new-export-control-law/ (noting that through this law, "exports and transfers of products, technology, and services may be prohibited or subject to licensing requirements based on the product features, end-users, destinations, or end-uses.").

[410] Henry Gao, *Data Regulation with Chinese Characteristics*, CENTRE FOR AI & DATA GOVERNANCE 1, 10 (2019), https://ink.library.smu.edu.sg/caidg/2, at 5, 27 ("The shift in regulatory focus closely follows the development of the Internet in China, where it started as a novelty that is confined to the ranks of tech-savvy geeks, then gradually expands

this process, the CAC has emerged as a powerful ministerial-level agency to regulate online content and data processing. Designated by the Cybersecurity Law and Personal Information Protection Law as a centralized regulatory authority, the CAC has further consolidated the power to regulate the Internet, govern data processing, and spearhead cyberspace governance, largely putting an end to previous turf fights among multiple authorities.[411]

However, the development of domestic Internet industry and information technologies seems far from a major concern of the CAC. Rather, its primary mandates and responsibilities are to ensure cybersecurity and prevent sensitive and undesired online content from appearing in domestic cyberspace.[412] Such a security-centered mindset and normative priority can partly explain China's stringent online censorship and filtering, as well as its strict restrictions on cross-border data flows.[413] As such, the CAC stands in stark contrast with the USTR (whose main duties are to make and enforce trade rules) and European DPAs (who are the guardians of European fundamental rights of data protection and privacy).

(D) Data Localization Subject to Limited Exceptions

In retrospect, the Cybersecurity Law, Personal Information Protection Law, and Data Security Law have built up a comprehensive legal framework to regulate China's data security and cross-border data transfers. If fully implemented, these laws would establish the default rules of data localization, subject to only limited exceptions under stringent conditions. In essence, this data governance framework embodies a security-oriented paradigm, characterized by relatively burdensome, inflexible, and costly mechanisms of cross-border data transfers as well as a predominant role of the CAC.

First, while protection of individuals' data privacy is a component of China's TPDF regulation, the latter's rules are primarily driven by national security concerns.[414] In a broader sense, cybersecurity (a pillar of national security) is an overarching normative goal that undergirds China's digitalization policies, as reflected from President Xi's dictum—"cybersecurity and informatization are two wings of one body, and two wheels of one engine."[415]

---

to the masses with the proliferation of softwares and apps catered to popular uses, and now permeates everyone's daily life from socialising, shopping to entertainment and education. Recognising the central role played by the Internet in the modern life, the Chinese regulators have shrewdly chosen to regulate data, which is the essence of cyberspace that powers everything, especially with the rise of big data and artificial intelligence.").

[411] *Id*., 8-10. Cai, *supra* note (*Jurisdictional Report*), 91. See Cybersecurity Law 2016, art. 8; Personal Information Protection Law 2021, art. 60.

[412] Gao, *supra* note, 28. See Cybersecurity Law 2016, art. 8.

[413] Gao, *supra* note, 28.

[414] Cai, *supra* note (*Jurisdictional Report*), 91. According to Yanqing Hong, a leading Chinese expert who drafted China's cross-border data transfers regulations, such TPDF rules were largely designed to "address the threats of data security and national security in the era of big data—massive amounts of data are controlled by the private sector, the accuracy and value of which may even surpass government data, and hostile forces may use such data to subvert the Chinese government, launch cyber-attacks and endanger Chinese national security." See Hong, *supra* note.

[415] Paul Triolo et al., *Xi Jinping Puts "Indigenous Innovation" and "Core Technologies" at the Center of Development Priorities*, NEW AMERICA (May 1, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.

With such a security-centered mindset, China tends to frame TPDF rules as institutional tools to safeguard national security. In comparison, protecting data privacy and promoting cross-border economic flows become ancillary interests, subordinated to the primary goal of national security. As such, in China's security-oriented paradigm to regulate TPDF, the normative priority is to address data security threats and safeguard national security interests. Under the default rules of data localization, the burden is shifted to private-sector actors to justify that the proposed data exports would not endanger cybersecurity and national security, making TPDF a qualified exception on a *priori* defensive position.

Second, while China's data localization requirements are comprehensive and feature a broad scope of application,[416] not all data is treated equally. Rather, China adopts a risk-based approach to regulate TPDF, in that its regulatory interventions are meant to be commensurate with the relevant data's importance and the threats imposed to national security.[417] Normally, the bigger the risks arising from the data, the greater the regulatory restrictions imposed on TPDF.

In particular, China's internal data governance framework focuses on the security of CII and important data, treating them as the top priorities of its "categorical and hierarchical system" to protect national data security. Under China's conceptualization of national security, such priorities reflect the critical role of CII and important data to national and societal interests at large. As remarked by President Xi, "(CII) is the nerve center of the country's economic and social operations, and is the top priority for cybersecurity, and a target that is likely to draw the most advanced attacks."[418] Likewise, by introducing the concept of "important data" (which may include large sums of sensitive personal data), the Chinese approach aims at protecting a broad notion of security interests at the societal and national levels, encompassing cybersecurity, political and social stability, economic security, and public interests.[419]

By design, the presence of "CII" or "important data" may heighten the level of scrutiny, and their inherent risks posed to national security could make it more likely for the relevant data transfers to be prohibited or restricted. In contrast, for non-CII operators to export ordinary personal data whose volumes fall short of the CAC's thresholds, the regulatory scrutiny is typically much lower, especially if the exporters resort to the certification mechanism or standard contractual agreements.

Third, given China's risk-based approach to protecting data security and national security, the key problem then becomes how to evaluate the national security threats underlying TPDF. However, these risks are by no means easy to identify and calculate accurately. Some of the key factors to be evaluated in the security assessments—such as the "necessity" of the data exports, the risks arising from data transfers, and the impact of a receiving country's legal system on data security—are largely susceptible to regulatory authorities' subjective judgments, leaving plentiful room for

---

[416] Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (February 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.
[417] Hong, *supra* note.
[418] Yanqing Hong, *Designing Risk-Based Critical Information Infrastructure Protection in China*, RESEARCH ALLIANCE FOR DATA GOVERNANCE AND CYBER SECURITY (January 22, 2018), http://www.dgcs-research.net/a/Opinion/2018/0115/86.html (noting that President Xi made this comment at the Cybersecurity and Information Work Conference in April 2016).
[419] Hong, *supra* note.

discretion.[420] The same also goes for the definition and scope of "important data" and "CII", given the ambiguity of language and the incomplete enumerations of the Chinese regulations.[421] In light of the ample leeway for a judgment call, the CAC—with a primarily security-centered mindset—is empowered to exercise its discretion, for instance, to determine exactly which data should be subject to heightened scrutiny, and whether and how national security could be endangered. Therefore, implementation of this security-oriented paradigm to TPDF may largely depend on Chinese authorities' subjective perceptions of future-oriented risk factors, potentially featuring a relatively low level of legal certainty and predictability.[422]

Fourth, China's national security paradigm is characterized by a dominant role of the CAC. Unlike the previous sectoral patchwork lacking a centralized authority to regulate TPDF, the Cybersecurity Law fills this loophole by empowering the CAC to steer, co-ordinate, and supervise national regulatory activities on cybersecurity. Subsequently, the Personal Information Protection Law also designates this institution as a leading regulatory authority to spearhead personal data protection in China, placing nationwide data processing activities under its supervision and monitoring.[423] As a centralized super-agency, the CAC now wields consolidated regulatory authority to implement data localization and cross-border data transfer requirements. Thus far, the CAC has vigorously discharged its mandates to formulate ancillary regulations to implement the Cybersecurity Law, Personal Information Protection Law, and Data Security Law.[424]

On the enforcement side, the CAC is also endowed with sharpened sanctioning power. To discipline the breaches of the data localization requirements, they could exercise data embargo power to block outbound data transfers, and impose a fine up to five percent of a company's annual turnaround sum in the previous year.[425] Such an enhanced power helps to boost the CAC's role in securing law enforcement and corporate compliance.

Fifth, given that the Chinese data transfer mechanisms (i.e., security assessments, certification, and standard contractual agreements) are relatively onerous, inelastic, and costly, foreign firms whose business models rely on uninterrupted data flows may find it difficult to use them to freely transfer data on a routine and continuous basis. Rather, due to the time delays, legal risks, and compliance costs, they may have to localize the storage and processing of data by default.[426] In other words, under this national security paradigm, the restrictive requirements for cross-border data transfers may function as *de facto* measures of data localization.

On the other hand, foreign investments in information and communications technology (ICT) sectors are heavily regulated in China: thus far, only Chinese investors are allowed to operate data centers.[427] This means that foreign data operators have to cooperate with Chinese data centers to

---

[420] Cai, *supra* note (*Jurisdictional Report*), 91-92.
[421] Wei, *supra* note (Comprehensive but Ambiguous), *supra* note.
[422] See Cai, *supra* note (*Enforcing A New National Security?*), 70.
[423] Personal Information Protection Law 2021, art. 60.
[424] For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.
[425] Personal Information Protection Law 2021, art. 66.
[426] See Erie & Streinz, *supra* note, 31-32. For a detailed discussion, see *infra* chapter 5 ("China's Data Sovereignty"), section V.A.(C).
[427] Yao Chen et al., *New Construction Theme Series—The Admission and Investment Structure for Foreign Investors to Invest in China's Data Centers (I)*, ZHONG LUN RELEASES (July 16, 2020),

run local data storage business.[428] In this way, China's data localization requirements not only mandate "where" data is stored and processed, but also establish Chinese entities' ownership of and control over the relevant digital infrastructures.[429]

IV. ADAPTING CONCEPTUALIZATIONS AND PARADIGMS

So far, this chapter has focused on the Big Three's dominant conceptualizations of personal data and their primary approaches to regulating TPDF, which have shaped the basic contours of their governance models. With those in mind, it is worth noting that their conceptualizations and paradigms are dynamic and continuously evolving, rather than static and settled. Notably, the Big Three have been adapting their conceptualizations and regulatory approaches to accommodate each other, and to address the shifting balance of their defensive or offensive interests underlying TPDF. Rather than replacing their primary approaches, these recalibrations co-exist with the former, adding a newly formed layer of complexity to the global TPDF system. This Part provides a brief overview of this phenomenon.

A. THE U.S.

In the U.S.-China geopolitical rivalry, with the ever-narrowing gap in economic clout and technological strength between these two superpowers, the U.S. has increasingly framed China as a strategic competitor, which poses growing threats to its dominance, hegemony, and security interests.[430] With respect to Chinese investors, tech firms, and digital service providers, the U.S. has increasingly subscribed to a national security conceptualization of personal data, cautioning against security threats of digital surveillance, espionage, and misuse of personal data. With increasing invocations of national security grounds in trade and investment contexts, the U.S. has deployed foreign security screening, export controls, and administrative power to target Chinese companies as threat actors, whether in its domestic market or globally.

First, the U.S. has been increasingly tightening foreign investment screening of Chinese firms' acquisition of U.S. assets involving sensitive personal data, on the ground that foreign access to and control of such data could undermine its national security. On this basis, CFIUS has not been hesitant in unwinding Chinese firms' acquisitions of U.S. assets involving sensitive personal data, including sensitive data about LGBTQ people and the public's health records.[431] In 2020,

---

http://www.zhonglun.com/Content/2020/07-16/1612138555.html (noting that under both China's WTO commitments and its Foreign Investment Negative List (an ancillary regulation to implement Chinese Foreign Investment Law), the telecommunication services open to foreign investors do not contain the operation of data centers—but China has committed to opening this sector to investors from Hong Kong and Macao, though with strings attached on ownership). Wei, *supra* note.

[428] For instance, Apple has established a local data center with a Chinese digital company in Guiyang to store the data of its Chinese iCloud users locally. This is also the case of Airbnb. *See Inside Apple's Compromises in China*, NEW YORK TIMES (July 17, 2021), https://www.nytimes.com › apple-china-censorship-data; see also, Vicky Huang, *Airbnb Will Store Personal Data of China Users Locally*, THE STREET (November 1, 2016), https://www.thestreet.com/investing/airbnb-will-store-personal-data-of-china-users-locally-13875980. For a discussion on foreign companies' responses and concerns, see Wei, *supra* note.

[429] Erie & Streinz, *supra* note, at 32.

[430] Roberts et al., *supra* note, 661-662; Slawotsky, *supra* note, 10.

[431] See eg. Klint Finley, *US Is Forcing a Chinese Firm to Sell Gay Dating App Grindr*, WIRED (March 27, 2019), https://www.wired.com/story/us-forcing-chinese-firm-sell-gay-dating-app-grindr/. (based on national security

following a national security review by CFIUS, then President Trump issued an executive order, requiring ByteDance (the Beijing-based parent of TikTok) to divest its TikTok subsidiary in the U.S.[432] To justify its actions, the Trump administration argued that the Chinese government can clandestinely compile Americans' data through TikTok, and may use such data to blackmail U.S. targets, censor American speech, and disseminate propaganda, thereby compromising U.S. national security interests.[433]

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) has further strengthened CFIUS' authority to screen foreign investment on national security grounds. As a notable revision, FIRRMA has expanded CFIUS's jurisdiction to cover transactions of critical technologies, critical infrastructure, and sensitive personal data of U.S. individuals ("a TID US business").[434] Under its rules, a mandatory review is now required for transactions that would result in a foreign government-owned investor's acquisition of a substantial interest in a TID U.S. business.[435] When vetting foreign investment, CFIUS is empowered to consider a potential investment's effects on cybersecurity vulnerability (particularly with respect to meddling in U.S. elections), and on U.S. capability to meet national security requirements.[436] As to a proposed acquisition, the CFIUS also may assess the extent to which the investment could expose sensitive personal data of U.S. citizens to a foreign entity (public or private), which may exploit those data to undermine U.S. national security.[437]

Second, based on national security concerns, the U.S. has also been vigorously invoking its export control mechanisms to impose economic sanctions on leading Chinese tech firms with an edge on ICT services. By leveraging its dominant influence over key nodes in the global manufacturing networks, the U.S. has been ratchetting up export bans to cut off Huawei's supply chains of semiconductors, both domestically and globally.[438] While these moves have been critiqued by

---

concern with Chinese ownership, CFIUS forced Beijing Kunlun Tech, a Chinese firm, to sell its equity in Grindr (a gay dating app having access to sensitive consumer data, including sexual orientations, geolocation, and HIV status); Christina Farr & Ari Levy, *The Trump Administration Is Forcing This Health Start-Up That Took Chinese Money into A Fire Sale*, CNBC (April 9, 2019), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html (CFIUS cracked down upon an Chinese investor's acquisition of a US health start-up having large volumes of health data of Americans).

[432] PRES. PROC. NO. 10,061, 84 FED. REG. 51,295. But in subsequent judicial proceedings, the federal courts enjoined the TikTok ban, such that the CFIUS divestiture order was not enforced. See Chander & Sun, supra note, at 32.

[433] *TikTok Inc. v. Trump*, 490 F. SUPP. 3D 73, 77 (D.D.C. 2020). See also *Misty Hong v. Bytedance, Inc.*, 2019 WL 6481689, Case 5:19-cv-07792-SVK (N.D.CAL.) (Trial Pleading), para. 1 (claiming that "TikTok clandestinely has vacuumed up and transferred to servers in China vast quantities of private and personally-identifiable user data that can be employed to identify, profile and track the location and activities of users in the United States now and in the future.")

[434] FIRRMA 2018, Section 1704(4). "Critical infrastructure" refers to a "system or asset, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on national security." See FINSA 2007, Section 2(6).

[435] FIRRMA 2018, Section 1706, IV(BB).

[436] FIRRMA 2018, Section 1702(c)(4) and (6).

[437] FIRRMA 2018, Section 1702(c)(5).

[438] Bien Perez, *Inside China Tech: US Sanctions Leave Huawei All Shook Up*, SCMP (August 22, 2020), https://www.scmp.com/tech/big-tech/article/3098329/inside-china-tech-us-sanctions-leave-huawei-all-shook (noting new rules of US Commerce Department blocking Huawei's "ability to buy semiconductors, developed or produced using US technology, from anywhere", tightening its "avenues for sourcing critical chips to power its 5G base stations, smartphones and cloud computing business"). Farrell and Newman, *supra* note, 11-12.

many as protectionist moves, the U.S. government's justification is security-oriented. Namely, the U.S. has to act to guard against severe national security threats, since Huawei's economic and technological dominance in the global 5G networks could result in unprecedented capacities to surveil personal data and other digital information.[439]

Third, the U.S. has been consistent in wielding administrative power to ban the roll-out of Huawei's 5G telecommunication networks.[440] Likewise, the Trump administration issued executive orders to block and restrict the operation of Chinese social media platforms TikTok and WeChat.[441] While declaring social media apps as national security threats seems novel (if not far-fetched) for a superpower, the underlying logic is the same with the cases of Huawei and Didi: the immense data collection capacities could enable a foreign firm, and by implication, a foreign government, to access and control huge amounts of U.S. citizens' personal data and sensitive information. Not only could such data be combined with other data sets to reveal the government's classified and sensitive information, but it also enables assorted strategic moves, including coercion, blackmailing, censorship, and dissemination of anti-American propaganda.[442] However, following this logic, it might be difficult to draw a clear-cut line as to where such security threats end. Given the omnipresence of the Internet and Internet-of-Things in the digital era, all systems, products, devices, services, and technologies connected to the Internet may threaten national security, since they could, to varying degrees, collect, process, use, and exchange personal data.[443] Thus, we may continue to see more and more security-oriented regulatory measures show up, aimed at protecting sensitive personal data from suspicious foreign hands.

In short, while the trade-based paradigm remains the dominant U.S. approach to TPDF, on the home front, the U.S. has adapted domestic regulations to balance its defensive interests underlying potential data transfers, particularly with respect to its economic competitor and strategic rival—China. In that context, the U.S.—though formerly and often still a champion of the liberal international economic order—has been increasingly deploying a security-oriented conceptualization and paradigm to fence off national security interests underlying personal data, thus somehow converging to China's style of play.

B. The EU

Similar to the U.S., the EU also grows increasingly cautious over the national security risks imposed by large troves of personal data held by foreign firms. Though European data protection

---

[439] David Shepardson et al., *U.S. Moves to Cut Huawei off from Global Chip Suppliers as China Eyes Retaliation*, REUTERS (May 15, 2020), https://www.reuters.com/article/us-usa-huawei-tech-exclusive-idUSKBN22R1KC (according to a senior Commerce Department official: "This action puts America first, American companies first, and American national security first.").

[440] Cassell Bryan-Low et al., *Special Report—Hobbling Huawei: Inside the US War on China's Tech Giant*, REUTERS (May 21, 2019), https://www.reuters.com/article/us-huawei-usa-5g-specialreport-idUSKCN1SR1EU.

[441] Press Release, *U.S. Dep't of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States* (Sept. 18, 2020); Press Release, *U.S. Dep't of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States* (Sept. 18, 2020). See Jeanne Whalen et al., *US Bans WeChat, TikTok as China Becomes Major Focus of Election*, WASHINGTON POST (September 18, 2020), https://www.washingtonpost.com/technology/2020/09/18/tiktok-wechat-ban-trump/.

[442] See *TikTok Inc. v. Trump*, 490 F. SUPP. 3D 73, 77 (D.D.C. 2020).

[443] Slawotsky, *supra* note, 50-51 ("any products using a computer or services that use a computer and/or are connected to the internet are almost "automatically" potentially a point of data transfer").

law (exemplified by the GDPR) helps to mitigate such a threat, this fundamental rights-based paradigm provides no panacea for eradicating all national security risks arising from European data stored overseas.

First, the EU is concerned that its member states generally do not own internationally competitive cloud infrastructures where its citizens' personal data is stored and processed.[444] While the GDPR's extraterritorial application[445] can help to attenuate such data security concerns, for European personal data stored at cloud servers in a foreign jurisdiction (mostly, the U.S.), resolving the choice-of-law problem may be difficult and controversial, resulting in legal uncertainties and less clear-cut outcomes. Particularly, if that foreign jurisdiction keeps a track record of pervasive intelligence surveillance practices without being effectively checked by rule-of-law institutions, the EU's national security threats would loom prominently.

For this reason, German Chancellor Angela Merkel called the EU to strengthen its "digital sovereignty" by nurturing its own platforms to store and process data, while decreasing its reliance on U.S.-based tech giants.[446] As defined by the German government, "digital sovereignty" refers to the capacity of the government to maintain "independent self-determination" with respect to "the use and structuring of digital systems" and the data stored and processed by them.[447] Under this notion, relying on foreign-located cloud infrastructures to store and process European data translates into losing part of the EU's digital sovereignty.[448] Germany's stance echoed the alarm sounded earlier by France about the loss of sovereignty to foreign tech giants (especially with respect to cloud computing),[449] as well as the French call to strengthen its "sovereign cloud" and "build a France of digital sovereignty."[450]

Driven by national security concerns and the notion of "digital sovereignty", the EU has been building a European cloud computing initiative (the "Gaia-X" project) to store and process Europe's data (including personal data and governmental data), aimed at establishing "a secure

---

[444] Aaronson, *supra* (Data Is Dangerous), at 17-18.

[445] See e.g., GDPR, art. 3 (detailing the GDPR's scope of extraterritorial application).

[446] Guy Chazan, *Angela Merkel Urges EU to Seize Control of Data from US Tech Titans*, FINANCIAL TIMES (November 13, 2019), https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca. *Together for Europe's Recovery: Programme for Germany's Presidency of the Council of the EU 2020*, at 8, https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf ("(Germany)... want to establish digital sovereignty as a leitmotiv of European digital policy").

[447] Aaronson, *supra* note (Data Is Dangerous), 18 (citing Federal Ministry of Economic Affairs and Energy, Project Gaia-X, https://www.bmwi.de/Navigation/DE/Home/home.html).

[448] Chazan, *supra* note (noting that "Peter Altmaier, economy minister, said the data of companies such as Volkswagen, and that of the German interior ministry and social security system, were increasingly stored on the servers of Microsoft and Amazon. 'And in this we are losing part of our sovereignty.'").

[449] Chander & Sun, *supra* note, 15 (noting that "(a)s early as 2010, the French government was sounding the alarm about the loss of sovereignty in the face of foreign technology firms. François Fillon, then Prime Minister, observed that with respect to cloud computing, 'North Americans dominate this market, which nevertheless constitutes an absolutely major stake for the competitiveness of our economies, for sustainable development and even, I dare say it, for the sovereignty of our countries.'").

[450] *Id.* ("Among the strategies the government adopted was the promotion of 'le cloud souverain'—the 'sovereign cloud'—through partnerships with cloud computing enterprises to support domestic employment, among other goals. In 2013, the French government detailed efforts to 'build a France of digital sovereignty,' including the desire to make to 'make France the world leader' in the field of 'Big Data.'").

and trustworthy data infrastructure for Europe."[451] As such, the hope is that the EU could make sure that the locally stored and processed data would be governed by EU data protection law, thus safeguarding national security interests and reclaiming its digital sovereignty.[452]

Second, the EU does not own as many national champions in digital technologies and telecommunication infrastructures as the U.S. and China do. Heavily relying on foreign suppliers of digital infrastructure (such as 5G) and critical technologies imposes cybersecurity and national security risks, particularly those arising from foreign intelligence surveillance and "weaponized interdependence".[453] In response, the EU sought to strengthen foreign investment screening mechanisms to maintain strategic independence in transformative technologies and digital infrastructures, and to secure data security and national security.

On the EU level, the EU Investment Screening Regulation sought to establish a pan-European institution to coordinate the screening of foreign investment that is likely to affect national security or public order.[454] Notably, the EU has expanded the scope of national security to include threats to its "strategic assets", which are defined as "fundamental interest of society" that is "crucial to Europe's security, and part of the backbone of its economy".[455] Stressing the importance of safeguarding the EU's security, public order, and its "strategic assets", the EU urged its member states to consider the potential effects of foreign investment on critical infrastructures, critical technologies, dual use items, as well as the access to and control of sensitive personal data, particularly when the foreign investor is controlled by a government.[456]

Further, on the member state level, a growing number of EU countries (most notably, Germany and France) have been establishing or strengthening foreign investment screening mechanisms. The focus is to safeguard national security interests underlying their critical infrastructures, critical technologies, and sensitive data from takeovers by foreign actors (particularly, Chinese investors—whether public or private).[457]

---

[451] *Id.*

[452] Aaronson, *supra* (Data Is Dangerous), at 18.

[453] Chazan, *supra* note (noting that the French president Emmanuel Macron said that if EU's companies continued to rely on US and Chinese manufacturers on digital infrastructure projects (such as 5G), "in 10 years' time, no one will be able to guarantee the technological soundness of your cyber-systems, no one will be able to guarantee who processes the data, and how, of citizens or companies.")

[454] European Commission, *EU Foreign Investment Screening Regulation Enters into Force*, PRESS RELEASE (April 10, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2088 (this framework allows the Commission to issue opinions when a foreign investment creates a threat to EU's security and public order).

[455] European Commission, *Guidance to the Member States Concerning Foreign Direct Investment and Free Movement of Capital from Third Countries, and the Protection of Europe's Strategic Assets, Ahead of the Application of Regulation (EU) 2019/452*, https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158676.pdf.

[456] Regulation (EU) 2019/452 of the European Parliament and of the Council, March 19, 2019, art. 4, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN.

[457] See eg. *Foreign Direct Investment Rules in Selected European Countries—An Overview*, DEBEVOISE & PLIMPTON (June 16, 2020), https://www.debevoise.com/insights/publications/2020/05/foreign-direct-investment-rules-in-selected. See also Neil Cuninghame et al., *Corporate & Competition Updated 21 May 2020 Global Foreign Investment Control Regimes–Changes in light of COVID-19*, ARHURST (May 21, 2020), https://www.ashurst.com/en/news-and-insights/legal-updates/global-foreign-investment-control-regimes---changes-in-light-of-covid-19/#.

In sum, while its primary approach to regulating TPDF remains the fundamental rights-based paradigm, the EU has been increasingly embracing a security-oriented conceptualization and paradigm to balance its rising national security interests underlying personal data and digital technologies. In that regard, the EU's responses are more nuanced. With respect to the U.S., the EU's national security concerns focus on the protection of European data stored in U.S.-based cloud infrastructures against foreign intelligence surveillance, perceiving such an asymmetrical reliance on American digital giants as creating security vulnerabilities that could be targeted and weaponized. In response, the EU seeks to develop its own digital infrastructures to ensure that the storage and processing of important and sensitive European data would be subject to its own laws. Regarding China, the EU strives to ratchet up foreign investment screening mechanisms to address national security risks underlying personal data and data-driven technologies. Either way, the EU—increasingly aware of its growing defensive interests—has been adapting its conceptual framings, regulatory measures, and policy responses, in efforts to safeguard national security and maintain strategic independence on transformative technologies and digital infrastructures.

C. China

While China's policy priority for TPDF regulation is to protect national security and cybersecurity at the home front, the Chinese government increasingly subscribes to an economic conceptualization of personal data, emphasizing the crucial role of data for the development of the digital economy.

Elevating big data to the top of its domestic economic agenda, China has recently come to underscore the importance of data as a strategic resource, a digital capital, and a novel factor of production. Such an economic conceptualization is evident from China's Thirteenth Five Year Plan and other top-level governmental policy instruments guiding national economic and social development.[458] As put by President Xi, "in the Internet era, data is a new factor of production, a fundamental strategic resource, as well as the source of production capacity…. Therefore, China will build a digital economy relying on data as a key factor of production."[459] Thus, as a matter of national industrial policy, China aims to implement a "national big data strategy", leveraging big data as "a fundamental strategic resource" to "transform and upgrade domestic industries".[460] Also, China's "Made in China 2025" initiative strives to develop internationally competitive national

[458] The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China 2016-2020, https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf (Chapter 27: Implementing a "national big data strategy"). See Hong, *supra* note (noting that in the regulations and top-level policy instruments guiding China's economic and social developments, data (and big data) has been categorized as "basic strategic resources", aligned with "rare earth, oil, natural gas, minerals, forests".).

[459] *The Central Government Enacted the First Instrument on Market Allocation of Factors of Production, What Does It Mean?,* ECONOMICS DAILY (April 10, 2020), http://zw.china.com.cn/2020-04/10/content_75916618.html (noting that for the first time, data has been categorized as a factor of production in the central government's guiding economic instrument).

[460] The 13th Five-Year Plan, chapter 27 ("We will make big data a *fundamental strategic resource* and fully implement a plan for its development, accelerating the opening, sharing, development, and application of *data resources* so as to help transform and upgrade industries.") (emphasis added).

champions in cutting-edge technologies and data-driven industries, thus driving China up the global value chain.[461]

At present, such an economic framing of data has driven China to build a unified domestic digital market to promote free data flows across different regions within its borders, so as to better exploit the economic interests of big data.[462] Given China's immense domestic market and a 1.4 billion population base, the commercial potential of unrestricted domestic data flows is substantial. With respect to cross-border data flows, China has also been adapting its regulatory approach, seeking to accommodate its rising economic interests underlying personal data.

On the international level, supplying Chinese-built digital infrastructures to emerging markets in numerous Asian, Eurasian, and African countries is an essential component of China's Belt and Road Initiative ("BRI"), constituting a "Digital Silk Road" that dovetails with the "Made in China 2025" plan.[463] As suppliers of digital infrastructures and technologies, Chinese firms have been increasingly gaining access to a multitude of overseas data for commercialization. Given the burgeoning economic interests in commodifying rich troves of foreign personal data, China recently began to embrace an adapted trade-based approach to facilitate TPDF. This is evinced in the Regional Comprehensive Economic Partnership ("RCEP"), which was signed by China in November 2020. A mega-regional PTA, RCEP adopts a seemingly paradoxical "*binding-yet-unenforceable*" approach to regulating TPDF.

In the past, traditional Chinese PTAs have consistently used only aspirational language in their e-commerce chapters, and consciously avoided dealing with cross-border data transfer issues altogether.[464] But this position was radically changed in RCEP. Modelled on TPP's template of digital trade rules, RCEP contains *binding* rules for free data flows and against data localization.[465] Not only does RCEP oblige states not to "prevent cross-border transfer of information by electronic means", but it also prohibits states from localizing computing facilities.[466] This marks the first time that China has committed to binding obligations on TPDF in PTAs.

Regarding data privacy protection, RCEP merely requires the existence of any domestic legal or regulatory framework to protect e-commerce consumers and personal information, without an eye

---

[461] State Council's Notice to Enact "Made in China 2025", Guo Fa [2015] No. 28 (May 19, 2015), http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm. Erie & Streinz, *supra* note, 22, 48 (noting that "[t]he (Digital Silk Road) dovetails with such initiatives as the 'Made in China 2025' plan, which aims to drive China up the global value chain by producing 'smart' manufacturing, and which in 2020 received a boost of $1.4 trillion.").

[462] On the central Chinese government's policy papers articulating the goal of establishing a unified national digital market where data could free flow across different regions, see State Information Center, *The Systemic Structure and Implementation Methods of Mega-Scale Data Factor Market Led by A National Unified Big Data Center*, STATE INFORMATION CENTER'S PRESS RELEASE (July 15, 2021), http://www.sic.gov.cn/News/609/11005.htm; State Information Center, *Dong Shu Xi Suan: Study on the Overall Framework of China's Cross-Regional Data Flows and Implementation Methods*, NATIONAL DEVELOPMENT AND REFORM COMMISSION'S PRESS RELEASE (March 27, 2020), https://www.ndrc.gov.cn/xxgk/jd/wsdwhfz/202003/t20200327_1224296.html?code=&state=123.

[463] Erie & Streinz, *supra* note, 2, 4, 48.

[464] Thomas Streinz, *RCEP's Contribution to Global Data Governance*, AFRONOMICSLAW (February 19, 2021), https://www.afronomicslaw.org/category/analysis/rceps-contribution-global-data-governance-0.

[465] *Id.*

[466] RCEP, arts. 12.15(2), 12.14(2).

for the substance of such a system.[467] Aligned with TPP, this approach treats data privacy protection as a matter of consumer protection anchored in the market's domain, while permitting no scrutiny over the merits of such a framework. This permissive "privacy floor" reflects an economic conceptualization of personal data, framing data privacy protection as an instrumental tool to achieve prioritized trade interests—rather than as intrinsic human rights in and of themselves.

However, when designing the public policy and security exceptions to binding TPDF commitments, RCEP substantially deviates from TPP by allowing far greater regulatory leeway for states to adopt restrictive measures that they "*consider necessary*". For the legitimate public policy exception, RCEP stipulates that the "necessity" of the measures is to be decided by the host state itself, diverging from TPP's objective "necessity" test that will scrutinize whether the restrictions are greater than necessary to achieve the policy goal.[468] Instead, the claimant state may only challenge whether the measures are applied arbitrarily or discriminatorily, or constitute a disguised restriction on trade. Further, under a self-judging national security exception clause, measures that a state "considers necessary for the protection of its essential security interests" are immunised from being disputed altogether.[469] Finally, while TPP subjects data restrictive regulations to both state-state dispute resolution and investor-state dispute resolution mechanisms, RCEP directly precludes this possibility. For any disputes arising under the e-commerce chapter, member states should resort to good-faith consultations with each other; alternatively, they may refer the matter to the RCEP Joint Committee.[470] In this way, RCEP's TPDF commitments become judicially *unenforceable*.

In short, RCEP not only incorporates TPP's binding commitments to advance free data flows, but also substantially mitigates them by retaining broad and sweeping carve-outs to safeguard states' regulatory autonomy—such that these obligations become "*binding-yet-unenforceable*".[471] To the extent that it suggests which PTA provisions are acceptable to China, RCEP serves China's important interests on two major fronts.

First, the self-judging "essential security interest" exception enables China to effectively immunise its security-oriented paradigm to regulate TPDF from international dispute resolution. Thus, at the home front, China's domestic data governance framework remains unchecked from external scrutiny, accommodating its predominant national security interests underlying personal data.

Second, the binding data flow commitments enshrined in RCEP could incentivize and facilitate inbound data transfers, allowing China to increasingly access and commercialize overseas personal data harvested by Chinese firms (especially along the Digital Silk Road). Undergirded by China's rising economic conceptualization of personal data, this "mitigated" trade-based approach brings into play the economic logic underlying personal data: by facilitating cross-border data flows, it

[467] RCEP, arts. 12.7, 12.8. See TPP, art. 14.8. See Streinz, *supra* note (RCEP).
[468] RCEP, arts. 12.15(2), 12.14(2).
[469] *Id.*
[470] RCEP, art. 12.17 (Though, RCEP leaves open the possibility for states to opt to apply state-state dispute resolution to disputes arising under this chapter, when they later review the agreement).
[471] Streinz, *supra* note (RCEP).

seeks to leverage data's economic interests, thus boosting the development of domestic digital economy and transformative technologies.

V. CONCLUSION

How a sovereign actor conceptualizes personal data and frames the TPDF system is often a complex, value-balancing process, given that different interests may feature a multi-dimensional relationship.[472] Yet, regarding the issue-area of TPDF, three primary conceptualizations of personal data canvassed in this chapter are predominant in the Big Three's regulatory policymaking, respectively, while gaining increasing dominance in global data governance discourses.

Divergent conceptualizations of personal data—as a factor of production, a human rights embodiment, and an element of national security—underpin three dominant approaches to regulating TPDF. The latter are an economic paradigm that focuses on maximizing the economic potential of data, a rights-based paradigm that prioritizes individuals' data privacy protection, and a security-oriented paradigm that privileges national security interests. While national and transnational regulatory rules that govern TPDF are still at the formation stage, these three regulatory approaches—each guided by a primary conceptualization and supported by a great power—come to "rise and rule" within the Big Three's respective regulatory "spheres of influence".[473]

Notably, adopting a conceptual framing could generate significant implications on how one understands the system's essential nature, designs its underlying logic, evaluates its normative legitimacy, and decides which interests or values should be prioritized and at what costs, leading to different legal and policy prescriptions for regulatory interventions. In this sense, behind divergent conceptualizations of personal data are a set of competing governance models, characterized by different policy priorities, normative justifications, substantive norms, as well as institutional structures. Devising rules to regulate TPDF requires a sovereign actor to choose one (or more) conceptualization(s) and regulatory approach(es) among an array of competing paradigms, in ways that would determine what constitutes the default rules and the exceptions.

In essence, the rising transnational economic, political, and societal tensions surrounding TPDF regulation often reflect the collision of three major conceptualizations and legal paradigms, which compete to claim authority to govern the decision-making process. Together, these three conceptualizations provide divergent answers to the questions of *who* should control *how* data

---

[472] For instance, despite the dominance of commercial interests, the economic framing of personal data also serves the U.S. government's national security interests, as free data flows facilitate U.S. national security authorities' signals intelligence and surveillance of data. For the EU, aside from pursuing normative value (which is paramount), a rights-oriented conceptualization of personal data also functions to safeguard national security interests against foreign intelligence surveillance, while achieving important economic goals (i.e., furthering EU market integration, and promoting internal data flows). In the case of China, while its national security interests largely determine a security-oriented framing, the latter may also be deployed to localize data to benefit domestic digital industry, while undermining foreign digital giants' competitive advantage. See *infra* chapter 3 ("EU's Forum-Shifting"), section II.B., section III.B.(A), and section IV; *infra* chapter 5 ("China's Data Sovereignty"), section III.B.; *infra* chapter 7 ("Conclusion"), section IV.C.

[473] See *infra* chapter 2 ("U.S.-led Regime- and Forum-Shifting"), Section III.D; chapter 4 ("Implications of EU Data Protection Law"), Section II; chapter 6 ("Policy Diffusion of the Chinese Approach").

flows on *what* terms in the global economy. How a sovereign actor conceptualizes what personal data is and what the TPDF system should be may result in not only different "optimal" balance struck among three major interests of personal data, but also divergent paradigms to institutionalize the fundamental choices and provide legal and regulatory solutions,[474] thereby shaping the pathway of the emerging global data governance framework.

[474] An exceptional case is the transatlantic data transfer arrangements, which enable the U.S. and the EU to find a compromise solution to accommodate their institutional differences with respect to data privacy protection. To facilitate data flows between their divergent internal data privacy regimes, the U.S. and the EU managed to come up with *sui generis* institutional arrangements to transfer European personal data for American companies. Such arrangements feature a voluntary "opt-in" mechanism for participating firms to self-certify their adherence to EU data protection standards, backed up by American and European authorities' oversight and enforcement. Caught between the economic and the rights-oriented conceptualizations of personal data, this transatlantic data transfer framework deploys mixed institutions to implement EU data privacy norms, creating an exception for the protection of EU-originated personal data in the U.S. See *infra* chapter 3 (EU Forum-Shifting), section IV.A.-B.

Chapter 2

U.S.-Led Regime- and Forum-Shifting— The Rise and Rule of a Trade-Based Approach to International Personal Data Transfers

Table of Contents

I. INTRODUCTION 88

II. EARLY REGULATIONS OF CROSS-BORDER PERSONAL DATA TRANSFERS: THE INSTITUTIONAL *STATUS QUO ANTE* 90

III. STAGE ONE: HORIZONTAL REGIME SHIFTING AND THE WTO'S MULTILATERAL TRADE LAWMAKING 92

A. The Uruguay Round of Multilateral Trade Negotiations 92

B. How Is GATS Insufficient to Address Cross-Border Data Flows? 93

C. Post-GATS Rulemaking in the WTO 97

IV. STAGE TWO: VERTICAL FORUM-SHIFTING THROUGH PTAS 99

A. The U.S. Digital Trade Agenda 100

B. TPP, TTIP, and TiSA 103

(A) Strategic Fragmentation, Divide and Conquer, and Plurilateral-Minus-One 103

(B) Evolution of Digital Trade Provisions from KORUS to TPP 105

(a) Binding and Enforceable Commitments for Cross-Border Data Flows and against Data Localization 105

(b) Consumers' Data Privacy Protection 109

(C) TTIP and TiSA 110

C. USMCA, and Subsequent PTAs 111

(A) USMCA 111

(a) Stronger Commitments on Transborder Data Flows 111

(b) Consumers' Data Privacy Protection 112

(1) An Economic Approach to Data Privacy Protection 113

(2) Promoting a U.S. Model of Accountability Mechanism—the APEC CBPR System 114

(B) Subsequent Trade Negotiations 118

V. POLICY DIFFUSION 120

VI. CONCLUSION 122

I. INTRODUCTION

As the role of data gains increasing prominence in the global digital economy and becomes crucial for the development of cutting-edge technologies, regulatory battles among great powers to set the

rules for international personal data transfers increasingly intensify. Over the past three decades, there has been a notable proliferation of international, regional, and national rules to regulate cross-border personal data flows. These include international trade agreements, supranational or regional data privacy instruments, national laws and regulations, and private-sector self-regulatory mechanisms. Among these legal sources, there is a prominent trend that U.S.-promoted digital trade rules have been increasingly dominating the international trade regime over time, setting the regulatory standards on this issue-area for the rest of the world.

While legal scholarship on U.S.-led trade treaties governing cross-border data transfers abounds, absent from existing literature is a systemic, holistic analysis of what these discrete treaty provisions add up to in the aggregate as a regulatory model, how they evolve over time, as well as the implications for other countries' data governance policies. Drawing on IR scholarship on analysis of regime complexity, this chapter strives to fill this gap by reconceptualizing the U.S.-led trade-based approach to international personal data transfers. At the core, it explores how the U.S. has deployed the lawmaking strategy of regime- and forum-shifting to develop international rules in pursuit of its domestic trade agendas, shaping the international trade regime based on its policy preferences.

The existence of multiple rulemaking venues without a normative hierarchy or an overarching political authority enables sovereign actors—particularly superpowers—to adopt a lawmaking strategy of "regime-shifting" to shape the evolution of rules on their preferred terms. As a policy change strategy, "regime-shifting" strives to strategically relocate international treaty negotiations or lawmaking processes from an international venue to a parallel one where alternative policy priorities prevail, in efforts to alter the institutional *status quo ante*, redefine the larger political context, and ultimately reconfigure the entire system of rules.[475] While regime-shifting may take place across different international regimes at a horizontal level ("*horizontal regime-shifting*"), it also can occur within a particular regime ("*vertical forum-shifting*"). In the context of international trade law, "vertical forum-shifting" repositions the locus of "norm-setting, rule-making, implementation, and enforcement" to bilateral, plurilateral, regional fora below the multilateral level, in order to achieve the desired rules and policies.[476]

Through this analytic lens, the creation and development of U.S.-promoted data transfer provisions in international trade agreements can be understood as the result of continuous "horizontal regime-shifting" and "vertical forum-shifting" initiatives led by the U.S. In so doing, the U.S. sought to establish, anchor, and refine international trade rules that well serve its dominant domestic interest groups and align with its competitive advantage, shaping the international legal order based on its terms. By tracing the evolution of U.S.-led trade rules as such, this chapter charts the development of a trade-based approach to international personal data transfers, and demonstrates how the underlying economic and strategic motivations have shaped the legal and policy outcomes.

---

[475] Lawrence R. Helfer, *Regime Shifting: The TRIPS Agreement and New Dynamics of International Intellectual Property Lawmaking*, YALE J. INT'L L. 1, 14, 16 (2004). Karen Alter & Sophie Meunier, *The Politics of International Regime Complexity*, 7(1) PERSPECTIVES ON POLITICS 13, 16-17 (2009).

[476] Susan K. Sell, *TRIPS Was Never Enough: Vertical Forum Shifting, FTAs, ACTA, and TTP*, 18 J. INTELL. PROP. L. 447, 451 (2011).

Within the transnational regime complex, these provisions have been increasingly emulated in PTAs adopted by U.S. trading partners and beyond, representing a prominent set of "gold standards" for future digital trade and global data governance. This salient phenomenon of "policy diffusion" enables the U.S. to become an important global rule-maker to set the legal and regulatory requirements for transnational data transfers, bolstering its position in the international regulatory competition against other superpowers. Moreover, it empowers the international trade regime to make a strong claim against other competing regimes and institutions to govern cross-border personal data flows.

The remainder of this chapter proceeds as follows. Part II gives a brief overview of the institutional *status quo ante* preceding the U.S.' deployment of regime- and forum-shifting. Part III discusses the U.S.' *horizontal regime-shifting*, relocating the decision-making authority to govern cross-border data transfers from nascent international *privacy* instruments to the international *trade* regime. Part IV analyzes the U.S.' subsequent efforts of "*vertical forum-shifting*", using PTAs to set the terms for international data flows. Part V summaries with concluding remarks.

II. EARLY REGULATIONS OF CROSS-BORDER PERSONAL DATA TRANSFERS: THE INSTITUTIONAL *STATUS QUO ANTE*

In the 1970s and 1980s, advanced democracies adopted divergent regulatory approaches to protect data privacy, which can be broadly grouped into three categories. First, many European countries (including France, Germany, Luxembourg, Sweden, Denmark, Norway, and Austria) enacted a comprehensive data privacy legislation with relatively stringent rules in the public and private sectors.[477] These data protection rules are enforced by specialized, independent regulatory agencies, which are vested with delegated authority to fulfill their mandate.[478] Second, countries such as the U.S. and Switzerland adopted a sectoral, piecemeal approach to protect data privacy. While this regime has enforceable data privacy rules to protect individuals against the government, data privacy in the private sector is primarily regulated by firms through business self-regulation, with some legislations for select sensitive sectors.[479] Third, other countries, like Italy, Belgium, Greece, Spain, Portugal, simply did not have national data privacy laws at all.[480] By the mid-1980s, many national data protection laws in Europe authorized domestic regulatory authorities to block cross-border transfers of personal data, where the recipient country did not maintain an "equivalent" level of data protection.[481]

On the supranational level, there are two influential first-generation international data privacy instruments: the OECD *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (OECD Guidelines) (1980) and the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention 108) (1981).

---

[477] ABRAHAM NEWMAN, PROTECTORS OF PRIVACY 23-25, 26-30 (2008). A.C. Evans, *European Data Protection Law*, 29 AM. J. COMP. L. 571, 571-72 (1981).
[478] NEWMAN, *supra*, 26-28. LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 100-102 (2014).
[479] NEWMAN, *supra*, 30-35.
[480] Id., 35.
[481] Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 474-477 (1995).

The OECD Guidelines are a set of non-binding principles that member countries may enact to protect individuals' data privacy and regulate cross-border personal data transfers. Driven by the economic concerns that national data privacy regulations may be used to pursue protectionist purposes,[482] these Guidelines aim at two core goals: (i) to ensure certain minimum standards of data privacy protection in member countries, and (ii) to reduce, as far as possible, the need for governments to restrict international personal data transfers due to data privacy risks (and thus, to strengthen cross-border data flows).[483]

In addition to the provisions establishing principles of data privacy protection, the Guidelines contain the following main provisions to regulate cross-border data flows. First, the Guidelines call on member countries to "take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure."[484] Second, they require each member country to "refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation."[485] Third, the Guidelines impose a proportionality requirement: member states should "avoid developing laws, policies and practices in the name of protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."[486]

While the Guidelines embody the most widespread consensus on data privacy protection and cross-border data flow regulation at the time, two factors hinder their efficacy in achieving regulatory harmonization in national data protection laws. First, with a soft law nature, they are not legally binding on member countries. Second, the Guidelines were written at a high level, such that the relevant principles may be not prescriptive and precise enough. This leaves plentiful leeway for member countries to implement them in different ways in view of their own legal and regulatory systems. In fact, since the enactment of the Guidelines, transnational regulations of cross-border data flows has become more diverse, due to the growing differences in national and regional legal frameworks of data privacy protection.[487]

Neither does the Convention 108 provide a satisfactory institutional solution. An influential international treaty specifically addressing data protection, the Convention not only provides a set of core principles to protect data privacy, but also includes provisions to regulate cross-border data flows. [488] But it contains many gaps and limitations, which may cause problems for its implementation and undermine its effectiveness. These include the lack of rules for personal data transfers to a non-member country, the failure to set up independent oversight agencies responsible for its implementation and enforcement, and the relatively general and abstract formulations of

[482] BYGRAVE, *supra*, 44.
[483] OECD Privacy Framework, Explanatory Memorandum, para. 25. CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAWS 35 (2011).
[484] OECD Guidelines 1980, Part III, para. 16, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
[485] *Id.*, para. 17.
[486] *Id.*, para. 18.
[487] KUNER, *supra*, 36.
[488] Convention 108, arts. 4-10, 12.

core data protection principles.[489] In any event, the Convention failed to spur many European countries to enact national data protection laws, falling short of adequately harmonizing domestic regulations across Europe.[490] Also, given that its member countries were primarily European countries in the 1980s, the Convention was more of a European-wide instrument, rather than an agreement with universal and geographically representative membership.

In sum, enacted in the 1980s, the OECD Guidelines and Convention 108 represented nascent international efforts to develop regulatory rules to address the potential blockage of cross-border personal data transfers. However, both instruments were limited in their membership, lacked mandatory enforcement mechanisms, and did not substantially harmonize national regulations on data privacy protection and transborder data flows. This reflects the institutional *status quo ante*: by the late 1980s, while recognizing the need for facilitating cross-border data flows, policymakers around the world "did not agree on how, when, and where data flows could be restricted."[491]

In response, the thrust of the U.S.' efforts was to bring international data transfers into the international trade regime, using trade agreements to tackle threats of data export blockages. These initiatives can be grouped into two different stages, with one featuring horizontal regime shifting and the other focused on vertical forum shifting.

III. STAGE ONE: HORIZONTAL REGIME SHIFTING AND THE WTO'S MULTILATERAL TRADE LAWMAKING

At this stage, the U.S. sought to shift the transnational lawmaking initiatives to the international trade regime, using the newly established multilateral trade rules to regulate cross-border data flows. The result of this round of lawmaking efforts is the establishment of the WTO. While the General Agreement on Trade in Services (GATS) extends international trade rules to govern trade in services and cross-border data flows, this legal framework is deficient in adapting to the rapid development of digital trade largely unanticipated by its drafters. Neither can these inadequacies be remedied by new multilateral trade negotiations.

A. The Uruguay Round of Multilateral Trade Negotiations

When the Uruguay Round of multilateral negotiations was launched in 1986, U.S. negotiators sought to create global trade rules to liberalize trade in services and address associated barriers.[492] Allying with the EU, the U.S. wielded asymmetrical power to effectively control the agenda-setting process and formulate the essential terms of the deal.[493] When closing this round, the U.S. and the EU not only threatened to exit the General Agreement on Tariffs and Trade 1947 (the

[489] BYGRAVE, *supra*, 38-41.
[490] Abraham L. Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, 62 INT'L ORGAN. 103, 109-110 (2008).
[491] Susan A. 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*, 14 WORLD TRADE REV. 671, 681 (2015).
[492] Juan A. Marchetti & Petros C. Mavroidis, *The Genesis of the GATS (General Agreement on Trade in Services)*, 22 EUR. J. INT'L L. 689, 692 (2011).
[493] Richard Steinberg, *In the Shadow of Law or Power? Consensus-Based Bargaining and Outcomes in the GATT/WTO*, 56 INT'L ORGAN. 339, 354-56 (2002).

predecessor of the WTO), but also pursued a single undertaking approach (ie., "nothing is agreed until everything is agreed") to present developing countries with a package deal of new WTO agreements.[494] Unwilling to lose access to the large markets of the U.S. and the EU, developing countries generally had no better alternatives than to join the deal on the terms largely set by the former.[495] The result is the creation of a multilateral trading institution (the WTO), as well as the conclusion of the GATS (a trade treaty dedicated to liberalizing trade in services).

In the Uruguay Round negotiations, U.S. financial sector played an indispensable role in pushing for the GATS.[496] Among domestic interest groups, American Express was pivotal in lobbying the United States Trade Representative (USTR) for multilateral negotiations on trade in services.[497] In the 1980s, American Express' business model "depend[ed] on the rapid transmission of large amounts of data across national borders through sophisticated computer and telecommunications networks."[498] Concerned with an increase of national data restrictive regulations in foreign markets, American Express pressed the USTR to conclude international trade rules that would secure global flows of financial data essential to its business model.[499] As such, in the process that created the GATS, the key goals of dominant U.S. business interest groups were to liberalize trade in services, prevent trade protectionism, and avoid local barriers to cross-border data flows.

B. How Is GATS Insufficient to Address Cross-Border Data Flows?

Compared with the previous status quo, GATS represents a major achievement. For the first time, it brings services into the ambit of international trading rules, which used to govern only trade in goods. [500] Indeed, this treaty is the primary multilateral trade agreement that contains comprehensive rules to liberalize trade in services across different sectors and modes of supply.[501] Within specified service sectors, member countries committed to providing market access and non-discriminatory treatment (among others) to service suppliers from other signatory countries.[502] And these rules are enforceable through the mandatory dispute settlement mechanism of the WTO.

To invoke GATS to discipline measures restricting cross-border data flows, the following provisions may be particularly relevant, to the extent that the categories of data affected correspond to service sectors or sub-sectors where the state undertakes specific obligations without relevant

---

[494] *Id.*, 357, 359-360.
[495] Richard Stenberg, *Judicial Lawmaking at the WTO: Discursive, Constitutional, and Political Constraints*, 98 AM. J. INT'L L. 247, 265 (2004) ("noting that the US and the EU "presented the developing countries with a fait accompli: either sign onto the entire WTO package or lose the legal basis for continued access to the enormous European and U.S. markets."). See LLOYD GRUBER, RULING THE WORLD: POWER POLITICS AND THE RISE OF SUPRANATIONAL INSTITUTIONS 47, 50-57 (2000).
[496] Marchetti & Mavroidis, *supra*, 692-693.
[497] *Id*., 693-694.
[498] *Id*., 694.
[499] *Id*. Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHICAGO L. R. (forthcoming 2023), at 14, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531.
[500] BERNARD M. HOEKMAN, THE GENERAL AGREEMENT ON TRADE IN SERVICES, IN THE NEW WORLD TRADING SYSTEM: READINGS (Paris: OECD 1994).
[501] GATS, art. I. Under this framework, signatory states agree to extend their obligations not only to suppliers who are present within their territory, but also to those who are offshore. Id.
[502] See e.g. GATS, arts. II (most-favored-nation treatment), XVI (market access), and XVII (national treatment).

qualifications. If a data restrictive measure alleviated data transfer restrictions for a particular country (but not others) or favored domestic services, it risks violating the most-favored-nation treatment or national treatment obligations.[503] When a state restricted or banned cross-border data flows in sectors where it made commitments, such a measure can breach the market access obligation.[504] Data restrictive measures of general application may also infringe on the domestic regulation obligation, if they impose unreasonable compliance requirements on foreign service suppliers.[505] Finally, the general exceptions of GATS can be invoked to safeguard measures pursuing certain public policy goals (including data privacy protection and cybersecurity).[506] Ideally and theoretically, the GATS rules could create an open, enabling environment to support cross-border data flows and facilitate digital trade, without constraining national governments from regulating the Internet to achieve legitimate policy objectives.[507]

Further, GATS also explicitly recognize the importance of cross-border data flows. In the Understanding on Commitments in Financial Services, member states commit not to "prevent transfers of information or the processing of financial information, including transfers of data by electronic means…. necessary for the conduct of the ordinary business of a financial service supplier."[508] Likewise, the GATS Annex on Telecommunications contains provisions that require member states to ensure cross-border data flows subject to necessary measures to protect data security and privacy.[509] These provisions largely reflect the needs of U.S. service sector interest groups that pushed for this treaty.

When evaluated in hindsight, however, GATS has not effectively dealt with trans-border data transfers and relevant regulatory challenges arising from contemporary technological developments and data-driven business practices.[510] While GATS was concluded in the pre-Internet era, modern digital economy has leapt far beyond what was contemplated by this treaty, making the unsuitability of its application increasingly glaring for four major reasons.[511]

First, unlike the General Agreement on Tariffs and Trade (that regulates trade in goods), GATS creates a much weaker set of commitments, in that many of its obligations are sector-specific, and designed to expand through WTO negotiations over time.[512] This explains why under the WTO framework, the distinction between goods and services is important, since a different

---

[503] Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH. 182, 199 (2017). See GATS, arts II, XVII.
[504] Mitchell and Hepburn, *supra*, 200-201. See GATS, art XVI.
[505] Mitchell and Hepburn, *supra*, 199-200. See GATS, art VI.
[506] Mitchell and Hepburn, *supra*, 201-205. See GATS, art XIV.
[507] Andrew Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World*, 22 J. INT'L ECON. L. 389, 398 (2019); L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, *in* RESEARCH HANDBOOK ON TRADE IN SERVICES 371-372 (Pierre Sauvé & Martin Roy eds., 2016).
[508] Understanding on Commitments in Financial Services, para. B.8, https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm.
[509] GATS Annex on Telecommunications, para. 5(c), (d), https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm.
[510] Andrew Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VANDERBILT J. TRANSNAT'L L., 1073, 1091 (2018); Mitchell and Mishra, Regulating (JIEL), 398.
[511] Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHIC. J. INT'L L. 263, 264 (2006).
[512] *Id.*, 270.

categorization results in a different set of treaty obligations and/or flexibilities.[513] But cross-border data flows often involve not only trade in services, but also trade in goods; and sometimes services can constitute an integral part of a good (such as the Internet-of-Things).[514] This can make the application of GATS particularly difficult, because segregating the "goods-related and services-related aspect of the measures" can be rather challenging.[515]

Second, the outdated structure of GATS is insufficient to effectively liberalize trade in services and regulate data restrictive measures.[516] Under this treaty, there is no *horizontal* commitment on cross-border data flows.[517] While its provisions are theoretically applicable to measures restricting international data transfers, GATS deals with the relevant policy challenges only in a partial, indirect, and rudimentary manner. On the one hand, application of the core legal obligations (such as non-discriminatory treatment and market access) is subject to sector-specific commitments undertaken by a state in its schedule.[518] WTO member states generally enjoy a high degree of autonomy to tailor their commitments and prescribe limitations with respect to a specific sector.[519] Thus, the legal obligations on transborder data flows under GATS are contingent on the specific commitments made by a state in different sectors. Also, while GATS contains rules on cross-border flows of data for services in financial and telecommunication sectors, digital services in other sectors (such as computer and related services, audiovisual services, and advertising services) are not covered.[520]

Further, it is difficult to classify most modern digital services under the Services Sectoral Classification List of GATS, which provides a reference point for countries to make legal commitments under this treaty.[521] As products of novel, cross-cutting business models, many digital services (such as Google, Facebook, WeChat, TikTok) today are multifunctional, and use multiple forms of services to function as comprehensive digital platforms.[522] These business sectors are enabled by technologies not envisioned when GATS was formulated. This is why GATS' classification parlance is outdated and difficult to interpret in the context of the Internet and Internet-of-Things, particularly in the absence of authoritative definitions in the classification text.[523] Also, given that a country's commitments on a specific service sector (or subsector) in its schedule are exclusive, a cross-cutting digital service has to be classified under one category (but

[513] Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEORGETOWN J. INT'L L. 407, 414 (2017). See Shamel Azmeh & Christopher Foster, *The International Trade Regime and the Quest for Free Digital Trade*, 22 INT'L STUDIES REV. 1, 5 (2019) (noting that for instance, "the EU maintains market access limitations on services such as audio-visual that enable quotas for local cultural content. By classifying newly digitized goods as services, the EU would be able to maintain its market access limitations on services").
[514] Mitchell and Mishra, *supra*, Regulating (JIEL), 398.
[515] *Id.*
[516] Mitchell and Mishra, *supra* (Data at Docks), 1088-93.
[517] *Id.*, 1093.
[518] *Id.*, 1088-89.
[519] *Id.*
[520] *Id.*, 1092.
[521] *Id.*, 1089-91 (noting that this classification is more than three decades old and thus "does not adequately represent business sectors of a digital economy.").
[522] *Id.*
[523] Hosuk Lee-Makiyama, *Cross-Border Data Flows in the Post-Bali Agenda*, *in* BUILDING ON BALI: A WORK PROGRAMME FOR THE WTO 163, 164 (Simon J. Evenett & Alejandro Jara eds., 2013). Wu, *supra*, 271-272.

not multiple categories) under the GATS framework.[524] This makes classification of modern digital services difficult, controversial and unsatisfactory, creating substantial legal uncertainties in applying GATS.[525]

Third, application of the GATS exceptions cannot effectively address prominent policy challenges underlying data restrictive measures. GATS contains two types of such clauses—art. XIV (general exemptions) and art. XIVbis (essential security exceptions)—yet neither provides satisfactory solutions. Notably, whether these exceptions could justify data restrictive measures often necessitates "an extensive and sophisticated legal analysis", requiring adjudicators to consider "the technical feasibility of the measure, the manner of operation of the measure, the extent to which other technical alternatives might be available to achieve equivalent levels of security and privacy, and the resources available domestically".[526] Given the intrusiveness and complexity of these inquiries, application of the GATS exceptions is highly uncertain and controversial.[527]

While art. XIV allows exemptions from GATS commitments on grounds of data privacy and consumer protection,[528] this leaves many important regulatory issues unaddressed. Indeed, this "privacy exemption" indicates that from the outset, WTO member states recognized the importance of privacy protection as a policy goal, and hence, carved out data restrictive measures pursuing this objective (subject to certain conditions).[529] However, GATS only safeguards the regulatory autonomy of states to adopt measures to protect data privacy, but does not ensure that all members adopt a robust framework on data privacy protection.[530] Also, though GATS permits members to choose a specific level of data protection, it does not address the trade barriers arising from variant national data privacy regulations.[531]

Given that data privacy protection is a precondition for open, stable, and secured cross-border data flows, addressing this policy challenge requires states to adopt regulations to protect personal data, and to develop mutually compatible data privacy frameworks. Atypical of the traditional trade realm, such regulatory issues, however, are not specifically dealt with by the WTO agreements.[532] According to leading commentators, by bracketing data privacy protection, GATS decided not to "engage with the question of how best to protect privacy amid a growing global trade in personal data," but "deferred to the future the difficult decisions on when a privacy measure that restrains trade is necessary or discriminatory".[533]

Fourth, neither does existing jurisprudence of the WTO Dispute Settlement Body (DSB) provide the much-needed clarity. In fact, member states have been reluctant to challenge domestic regulations restricting data flows before the DSB. This is not only due to the uncertainties and

[524] Mitchell and Mishra, *supra*, Data at Docks, 1090.
[525] *Id*., 1090-91; Burri, *supra*, Regulating (GJIL), 414.
[526] Mitchell and Mishra, *supra*, Data at Docks, 1094-1095.
[527] *Id*.; Neha Mishra, *The Trade: (Cyber)Security Dilemma and its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567, 572 (2020).
[528] GATS, art. XIV(c)(ii); see also GAT Annex on Telecommunications, para. 5(d).
[529] Mitchell and Mishra, *supra*, Regulating (JIEL), 399. Chander and Schwartz, *supra*, 7-8.
[530] Mitchell and Mishra, *supra*, Regulating (JIEL), 399.
[531] *Id*.
[532] *Id*., 397, 399.
[533] Chander and Schwartz, *supra*, 8.

limitations of the GATS framework, but also reflects the complex political economy of digital trade, given the cross-cutting nature of transborder data flows.[534] As such, WTO member states are uncomfortable with invoking uncertain WTO rules (as they currently stand) to adjudicate sensitive political issues (including data privacy, cybersecurity, Internet governance, and economic development) implicated in domestic data regulations.[535] Despite the utility of the DSB, creative judicial interpretations of existing rules by WTO adjudicators can by no means replace the political consensus required to reform the substance and structure of GATS.

C. Post-GATS Rulemaking in the WTO

In 1997, President Bill Clinton administration articulated a set of international principles to govern cross-border data flows—the Framework for Global Electronic Commerce—in order to create an enabling environment for e-commerce.[536] Prioritizing foreign market access for domestic firms, the Framework stated that the U.S. "supports the broadest possible free flow of information across international borders," and that this administration will work with key trading partners to ensure that differences in national regulations would not constitute "disguised trade barriers."[537] To that end, President Clinton directed the USTR to secure trade treaties to create a tariff-free Internet for e-commerce and make e-commerce a "seamless global marketplace"; and directed the Secretary of Commerce to develop "a uniform international commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide".[538] Also, this instrument stated that the U.S. will work with key trading partners to support the private sector to develop business self-regulation standards and technological solutions to protect online privacy, ensuring that "differing privacy policies around the world do not impede the flow of data on the Internet."[539] An influential policy instrument, this Framework guided the trade policy of two subsequent administrations: Presidents George W. Bush and Barack Obama adhered to its core principles, including a limited role for government intervention, a focus on business self-regulation, prioritization of free data flows across borders, and treating barriers to data flows as "digital protectionism".[540]

However, since the Uruguay Round, no substantial progress has been achieved to liberalize digital trade and facilitate cross-border data flows at WTO negotiations, as expected by the U.S.[541] In the Geneva Ministerial Conference in 1998, the WTO launched the "Work Programme on E-Commerce." Many issues discussed within that framework have not obtained a solution, or even a clarification.[542] An exception to this is the commitments made by WTO member states not to

---

[534] Mitchell and Mishra, *supra* (Data at Docks), 1096.
[535] *Id*.
[536] Aaronson and Leblond, *supra*, 254.
[537] William J. Clinton and Albert Gore, Jr., "The Framework for Global Electronic Commerce", https://clintonwhitehouse4.archives.gov/WH/New/Commerce/.
[538] *Id*.
[539] *Id*.
[540] Aaronson, *supra* (*Why Trade Agreements*), 682-83.
[541] Sacha Wunsch-Vincent & Arno Hold, *Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral Versus Preferential Trade Negotiations*, *in* TRADE GOVERNANCE IN THE DIGITAL AGE 179, 179 (Mira Burri & Thomas Cottier eds., 2012).
[542] *Id.*, 180 ("Even on simple issues such as establishing a permanent and clear duty-free moratorium on e-commerce, or confirming the applicability of WTO rules and commitments to electronically-traded services, no results have been achieved."). Azmeh and Foster, *supra*, 16.

impose custom duties on electronic transmissions (the "WTO Duty-Free moratorium on electronic transmissions").[543] The U.S. government was a leading force behind this moratorium.[544] As temporary measures, the moratorium was implemented to prevent custom duties from being imposed on the transmission of electronic information, rather than the content of such transmissions.[545] While it has been temporarily extended several times at subsequent ministerial conferences, this moratorium turns out to be insufficient to deal with the regulatory challenges on cross-border data flows.

First, the majority of data flow restrictions across different countries today are not custom duties, but rather behind-the-border regulatory measures, such as domestic data privacy laws and cybersecurity measures.[546] The moratorium fails to deal with these policy challenges. Second, the moratorium's exact scope of coverage is subject to disagreements and controversies. As the content of digital products is increasingly represented and transmitted through a set of digital codes via the Internet, it is typically difficult to distinguish a tax on the content of data (subject to members' commitments under GATS) and that on the transmission of data (prohibited by the moratorium).[547] Third, there is no agreement on a permanent duty-free moratorium on electronic transmissions, despite the U.S.' strong push to that effect.[548] Rather, subsequent renewals of this moratorium may be obstructed by potential political disagreements among WTO members; and developing countries, such as India and African countries, have voiced strong support for the proposition against this moratorium (for it would cause substantial tariff loses to them and may disproportionately benefit firms in developed countries).[549]

At the Doha Round of WTO negotiations, no significant developments have been made on e-commerce and digital trade after almost two decades since 2001. While seeking to further reduce barriers to trade in services, the Doha negotiations stalled without making much headway in creating new rules, due to significant disagreements between developed and developing countries.[550] In the 2017 ministerial conference, advanced economies—led by the U.S.—sought to move the mandate of the "Work Programme on E-Commerce" from discussions to negotiations to push for new trade rules, but some developing countries—particularly the African Group and India—staunchly opposed this change.[551] Specifically, negotiators of a small group of states within the African Group played a crucial role in this process. Through internal discussions and coalition-

[543] Azmeh and Foster, *supra*, 16.
[544] Aaronson and Leblond, *supra*, 254.
[545] Mitchell and Mishra, *supra*, Data at Docks, 1093.
[546] Aaditya Mattoo & Ludger Schuknecht, *Trade Policies for Electronic Commerce*, WORLD BANK DEVELOPMENT RESEARCH GROUP POLICY RESEARCH WORKING PAPER NO. 2380, 2000, at 4, http://documents.worldbank.org/curated/en/164411468767105932/pdf/multi-page.pdf.
[547] Mitchell and Mishra, *supra*, Data at Docks, 1093.
[548] Burri, Regulation (GJIL), 415.
[549] See e.g. Communication from the African Group, Work Programme on Electronic Commerce, Report of Panel Discussion on "Digital Industrial Policy and Development", WTO Doc. JOB/GC/133 (July 21, 2017); Communication from India and South Africa, "Moratorium on Customs Duties on Electronic Transmissions", WTO Doc. WT/GC/W/747 (July 13, 2018).
[550] James McBride & Anshu Siripurapu, *What's Next for the WTO?*, COUNCIL ON FOREIGN RELATIONS (December 13, 2021), https://www.cfr.org/backgrounder/whats-next-wto.
[551] Azmeh and Foster, *supra*, 16-17. See eg. Statement by the African Group, Work Programme on Electronic Commerce, ¶ 3.2, WTO Doc. WT/MIN(17)/21 (Dec. 6, 2017).

building, such states managed to reach a group-wide consensus.[552] Leveraging the one-country-one-vote decision-making rule of WTO negotiations, these countries then acted in concert at the multilateral venue, and blocked ministerial negotiations from making much progress in liberalizing digital trade.[553]

Unlike the Uruguay Round, this time the "single undertaking" approach of trade lawmaking procedure prevented progress from being made even in select areas where it might have been easier to reach a consensus.[554] Notably, the large and diverse membership of the WTO made it difficult for members with different policy preferences to agree on the broad Doha mandate.[555] Further, the U.S., the EU, and developing countries maintained strong, persistent divergence on several major regulatory issues, including cross-border personal data transfers.[556] As a result, multilateral rulemaking has been seriously undermined, with the WTO increasingly sliding towards irrelevance compared to other trade fora.[557]

IV. STAGE TWO: VERTICAL FORUM-SHIFTING THROUGH PTAS

With limited substantial progress on trade lawmaking in the WTO, the U.S. resorted to vertical forum-shifting, pushing for its preferred digital trade rules through bilateral, plurilateral, and regional PTAs below the multilateral level.

First, the U.S. can better leverage asymmetrical power derived from its market size at these fora to push for its preferred norm-setting and rulemaking, making PTAs an institutional avenue to secure rules that are difficult to achieve at the multilateral level.[558] Second, PTAs can function as a stepping stone towards multilateralism. Through PTAs, a superpower like the U.S. can achieve a group-wide consensus on trade lawmaking among countries that are more like-minded or more amenable to its influence, and thus, would boost its bargaining position in subsequent multilateral negotiations. Finally, advanced, high-standard PTA provisions could serve as a template for other economies to emulate in their own trade agreements, generating "policy diffusion" effect to get more foreign governments on board.

In short, vertical forum-shifting could allow the U.S. to sidestep the negotiating power of some developing countries (and, to a lesser extent, of the EU) in the WTO, and to use alternative institutional channels to reconfigure the international trade regime based on its preferences and interests.

---

[552] Azmeh and Foster, *supra*, 17.
[553] *Id*. (noting that this "ministerial concluded with a lukewarm statement for future activities, the renewal of the moratorium, and the continuation of the 1998 working group but with no further progress.").
[554] Congressional Research Service, *World Trade Organization: Overview and Future Direction*, October 18, 2021, at 30, https://sgp.fas.org/crs/row/R45417.pdf
[555] *Id.*
[556] *Id.*
[557] McBride and Siripurapu, *supra*; Burri, *supra*, Regulating (GJIL), 417.
[558] Azmeh and Foster, *supra*, 4. Jean-Frederic Morin, *Multilateralizing TRIPS-Plus Agreements: Is the US Strategy a Failure?*, 12 J. WORLD INTELL. PROP. 175, 176 (2009).

A. The U.S. Digital Trade Agenda

During the Bush administration (from 2001 to 2008), the U.S. was committed to a new approach to foreign economic policy, prioritizing bilateral and regional trade liberalization.[559] In 2002, the Congress granted the Bush administration a new trade promotion authority (TPA) to conclude PTAs, and encouraged the President to create new trade rules to facilitate e-commerce and reduce digital trade barriers. [560] By creating a fast-track authority to negotiate new trade treaties, the TPA set forth "a set of ambitious negotiation goals that formalize a new U.S. digital trade policy".[561] Believing that the U.S. would make little progress in WTO negotiations, the USTR, Robert Zoellick, focused on bilateral PTAs in the Bush-era trade negotiations.[562]

However, the Bush administration, just like the prior Clinton administration, did not anticipate that other countries were increasingly adopting restrictive measures to control the Internet within their borders under various policy rationales (including data privacy protection, social control, and domestic industrial development), and that some foreign firms were increasingly gaining ground on their U.S. counterparts.[563] While the Bush administration began to include e-commerce chapters in many U.S. PTAs, their language did not keep up with the fast-changing Internet-driven economy.[564] Through new PTAs, the Bush administration made some progress in getting US trading partners to agree to avoid erecting new barriers to digital trade and imposing local presence requirements.[565] But none of these agreements contained binding and enforceable rules on cross-border data flows; nor did they clarify when governments could restrict such flows.[566]

Since 2009, leading U.S. technology firms and numerous industry associations (that represent various groupings) have increasingly formed a strong alliance of business interest groups, which played an indispensable role in the formation of U.S. "digital trade agenda". Focused on interventionist Internet regulations in foreign markets, these actors actively lobbied the U.S. government to address these "digital trade barriers" through trade treaties, prioritizing issues of cross-border data flows.[567] With substantial spending on lobbying and campaign contributions, such actors became powerful political forces in Washington DC.[568] And as more digital firms' businesses went global, the focus of their lobbying efforts shifted from intellectual property (IP) and domestic e-commerce to international trade issues.[569] Notably, such business interest groups considered the trade regime as a desirable venue to address their policy challenges, due to the

---

[559] Aaronson, *supra* (*Why Trade Agreements)*, 683.
[560] *Id.* Sacha Wunsch-Vincent, *The Digital Trade Agenda of the U.S.: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization,* 1 AUSSENWIRTSCHAFT 7, 7 (2003) ["*Digital Trade Agenda*"].
[561] Vincent, *supra* (*Digital Trade Agenda*), 8-9.
[562] Aaronson, *supra* (*Why Trade Agreements)*, 683.
[563] Susan Ariel Aaronson, *The Digital Trade Imbalance and Its Implications for Internet Governance*, CIGI PAPERS No. 25 (February 2016), at 7, https://www.cigionline.org/sites/default/files/gcig_no25_web_0.pdf ["Digital Trade Imbalance"]. See Aaronson and Leblond, *supra*, 254-255.
[564] Aaronson and Leblond, *supra*, 254.
[565] Aaronson, *supra* (*Why Trade Agreements*), 684.
[566] *Id.*
[567] Azmeh and Foster, *supra*, 13-14; Aaronson and Leblond, *supra*, 255; Aaronson, *supra* (*Digital Trade Imbalance*), 7.
[568] Azmeh and Foster, *supra*, 13-14 (noting that during 2011 to 2018, Google/Alphabet, Amazon, Facebook, Microsoft, Apple were among the top spenders on lobbying among all corporate actors.)
[569] *Id.*

prospects of reaching binding international rules, the scale of membership, strong dispute settlement mechanisms, enforceability of commitments, as well as the previous success in including IP rules in international trade agreements.[570]

For instance, Google (Alphabet) published a white paper in 2010 to document broad-scale restrictions adopted by numerous foreign countries on cross-border data flows, calling for "new international trade rules under bilateral, regional, and multilateral agreements" to discipline such unfair trade barriers that restrict or disrupt free flows of online information.[571] Likewise, a 2012 report of the Business Software Alliance (BSA) argued that the U.S. should eliminate digital trade barriers as a key objective in its digital trade agenda.[572] While initially dominated by digital firms, these campaigns soon expanded to have service companies join forces, which saw the digital trade agenda as a way to ensure foreign market access to digitally delivered services and address the limited liberalization of services in the WTO.[573]

Such campaigns stemmed from and reflected the fact that more U.S. digital and services firms grew to become important global players in their businesses, with many being world champions. As they were increasingly dependent on overseas markets, foreign data restrictive measures governing their operations became more costly, burdensome, and problematic, threatening their business models.[574] In response, these firms called for the U.S. government to do a better job at disciplining and limiting "digital protectionism", with a focus on China's practices.[575] These campaigns were successful in convincing top-level U.S. trade policymakers that existing WTO rules did not fully contemplate emerging barriers to digital trade, and that the government should vigorously pursue a "digital trade agenda" to create an enabling environment for U.S. firms to thrive as they did in the past.[576]

Importantly, despite burgeoning trade deficits in general, digital industries are where the U.S. has long maintained significant trade surplus, and thus enjoyed a dominant competitive advantage in the global marketplace.[577] When pressing the state to protect and advance their commercial interests, these private-sector actors highlighted their strength as competitive exporters and industries of the future, linked their businesses to trade policymakers' primary policy concerns, and appealed to America's long-standing free trade ethos and a "free and open" view of the

---

[570] *Id.*, 15-16.
[571] Google, *Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information*, GOOGLE PUBLIC POLICY BLOG (November 15, 2010), https://goo.gl/9CGxam ["Google Paper"].
[572] Robert Holleyman, *Lockout: How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets*, BUSINESS SOFTWARE ALLIANCE TECHPOST (June 20, 2012), https://techpost.bsa.org/2012/06/20/lockout-market-access-report/.
[573] Azmeh and Foster, *supra*, 16.
[574] *Id*., 14-15. Aaronson, *supra (Digital Trade Imbalance*), 7.
[575] Azmeh and Foster, *supra*, 14. Aaronson, *supra (Digital Trade Imbalance*), 7.
[576] See e.g. United States Congress Senate Hearing, Nominations of Robert W. Holleyman II and Cary Douglas Pugh, July 16, 2014, https://www.govinfo.gov/content/pkg/CHRG-113shrg93277/html/CHRG-113shrg93277.htm.
[577] John Selby, *Data Localization Laws: Trade Barriers or Legitimate Response to Cybersecurity Risks, Or Both?*, 25 INT'L J. L. INFO. TECH. 213, 215-16 (2017). See e.g., U.S. International Trade Commission, *Digital Trade in the US and Global Economics,* Part 2 (August 2014), at 14, https://www.usitc.gov/publications/332/pub4485.pdf.

Internet.[578] In particular, their lobbying initiatives were effective in presenting their demands as a powerful solution to cure America's trade woes, create jobs for Americans, anchor a privileged position for the U.S. in the global value chain, and ensure its capability to effectively compete in the international arena.[579] By pitching their cause in ways capturing the imagination of top-level policymakers as politically feasible, such business interest groups essentially translated their private interests into a matter of public interests for the U.S.[580] Such political efforts, together with U.S. policymakers' concerns over America's declining technological advantage against rising strategic competitors (such as China) in the digital economy and global tech race, have anchored the "digital trade agenda" at the heart of U.S. trade policy for new trade agreements.[581]

In 2009, President Obama made the "digital trade agenda" a key part of U.S. trade policy, and determined to use international trade rules to address digital protectionism.[582] In 2015, Deputy USTR (Ambassador) Robert Holleyman stated in a speech that "the Obama Administration has made promoting the digital economy a key component of its digital trade agenda."[583] Notably, Holleyman articulated a set of "Digital Dozen principles", reflecting the Obama administration's priorities for its digital trade agenda.

Demonstrating the U.S. government's commitments to transforming international trade rules, the Dozen principles include (i) prevention of discriminatory and protectionist barriers to cross-border data flows, (ii) prohibition of forced localization of computing facilities and the requirements to build data centers in foreign markets, (iii) provision of enforceable consumer protections to build consumer trust online, among others.[584] According to Holleyman, such principles would become the "key components of the 21st century global trading system," and the U.S. government would push for the inclusion of them in the Trans-Pacific Partnership (TPP) and other future-generation trade agreements.[585]

These "Digital Dozen" principles largely reflect the "Silicon Valley Consensus", a set of policy prescriptions for digital economic development.[586] Believing that the best way to develop the

---

[578] See SUSAN K. SELL, PRIVATE POWER, PUBLIC LAW 99-100 (2003); Azmeh and Foster, *supra*, 14; Google Paper, 3-5.
[579] See SELL, 99-100; Azmeh and Foster, *supra*, 14; Google Paper, 3-5.
[580] See SELL, 99-100; Google Paper, 3-5.
[581] Svetlana Yakoleva, *Privacy Portection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416, 483-484 (2020) ["*Privacy Portection(ism)*"].
[582] Aaronson, *supra (Why Trade Agreements)*, 685; Azmeh and Foster, *supra*, 14.
[583] Robert Holleyman, *Remarks by Deputy U.S. Trade Representative Robert Holleyman to the New Democrat Network* ("Remarks"), USTR ARCHIVES, SPEECHES/TRANSCRIPTS (May 1, 2015), https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade. Prior to his service in this office, Holleyman was an industry lobbyist and the CEO of the BSA for thirteen years. See Azmeh and Foster, *supra*, 14.
[584] Holleyman, *supra* (Remarks); USTR, *The Digital Dozen*, May 1, 2015, https://ustr.gov/sites/default/files/USTR-The_Digital_Dozen.pdf.
[585] Holleyman, *supra* (Remarks).
[586] Thomas Streinz, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, in MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP 330 (Benedict Kingsbury et al. eds., 2019) ["Megaregulation"]. See Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639, 645 (2014) ["*Silicon Valley*"]. Relatedly, the "Washington Consensus" is a set of economic policy prescriptions, which is widely regarded as desirable reform proposals for developing countries in crisis, and which was promoted by Washington, D.C.-based economists from the IMF and World Bank. See John Williamson, *The Washington Consensus as Policy Prescription for Development*, Lecture delivered at the World Bank (JANUARY 13, 2004), https://perma.cc/4HXL-AGLC.

digital economy is to reduce the legal risks faced by digital firms and refrain from regulating new risks they introduce, the Silicon Valley Consensus endeavors to ensure that digital businesses would thrive in a regulatory and legal environment that minimizes governmental regulations (whether in name of data privacy or otherwise).[587] While recognizing that the digital economy may create negative externalities, the Silicon Valley Consensus considers that the best way to address such risks is to rely on business self-regulation and technological solutions, rather than prescriptive governmental regulations.[588]

In 2015, the Congress granted the Obama administration a new TPA mandate, providing the specific negotiating goals to "secure cross-border data flows" and "combat mandatory directives for local storage and processing of data."[589] Reflecting the role of the Internet as a fundamental international trading platform, these objectives transcend the negotiating goals about e-commerce under the Bush administration's TPA.[590] In 2017, the Congress established a bipartisan "digital trade caucus", aiming to protect digital trade from foreign governments' protectionism, promote free flows of data, and eliminate data localization requirements.[591]

B. TPP, TTIP, and TiSA

(A) Strategic Fragmentation, Divide and Conquer, and Plurilateral-Minus-One

Since 2008, the Bush administration initiated negotiations over the TPP with eleven trading partners in the Asia-Pacific region, in parallel to talks with the EU over the Transatlantic Trade and Investment Partnership (TTIP) that started a year ago.[592] The Obama administration doubled down on these negotiations in pursuit of "strong, high-standards trade agreements".[593] Through negotiations of these mega-regional trade agreements, the U.S. sought to combat and reduce various barriers to trade that were on the rise over time, while setting the rules for future global economy.[594] While this choice to pursue two parallel regional tracks outside the WTO is generally attributed to the failure of the Doha Round, there are important political dynamics in this strategy.

First, separate, secret negotiations of the TPP and TPIP in two parallel tracks (rather than an inclusive one) represent a "Machiavellian game" of the U.S. to intentionally create "fragmentation" in global trade rulemaking, preventing its trade partners from forming a united front against it.[595]

---

[587] Streinz, *supra,* 330; Chander, *supra* (*Silicon Valley*), 645.
[588] Chander, *supra* (Silicon Valley), 648-49.
[589] Holleyman, *supra* (Remarks).
[590] *Id.*
[591] DelBene, *Paulsen Launch Bipartisan Digital Trade Caucus*, PRESS RELEASE (May 1, 2017), https://delbene.house.gov/news/documentsingle.aspx?DocumentID=1861.
[592] Eyal Benvensti, *Democracy Captured: The Mega-Regional Agreements and the Future of Global Public Law*, 23 CONSTELLATIONS 58, 58 (2016) ["*Democracy Captured*"]. It bears noting that the TTIP negotiations were officially launched in 2013 during the Obama administration.
[593] Statement by the President on Senate Passage of Trade Promotion Authority and Trade Adjustment Assistance, THE WHITE HOUSE (May 22, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/05/22/statement-president-senate-passage-trade-promotion-authority-and-trade-a .
[594] Benvensti, *supra* (Democracy Captured), 58.
[595] *Id.*, 58-59.

Through this "divide and conquer" strategy, the U.S. was able to magnify its bargaining power to dominate the rulemaking process. In the TPP negotiations, other Asia Pacific countries were more heterogenous and divided than the EU, and thus, were less likely to unite against the U.S. In this context, negotiating "WTO-extra" and "WTO-plus" treatment across various economic sectors could create a competitive environment for these countries to join the pact, incentivizing them to make compromise to jump onto the bandwagon (as opposed to being left behind).[596]

In the TTIP negotiations, the EU, an otherwise economic rival to the U.S. in bilateral negotiations, was undercut by the parallel TPP track negotiated in secret.[597] Concerned that TPP (that can create a new model for future PTAs) might somehow discriminate against EU companies, the EU may feel more pressure to negotiate TTIP with the U.S.[598]

In this way, the U.S. strived to get around the one-country-one-vote system of the WTO, limiting the opportunities for weaker countries to build cross-issue coalitions to aggregate their bargaining power. By dividing and fragmenting its trade partners, the U.S. could take advantage of their economic dependencies and vulnerabilities, and better leverage its asymmetrical economic power derived from U.S. domestic market. As a result, this superpower is more likely to shape new trade rules based on its own interests, preferences, and visions.

Second, led by the U.S., the TPP negotiations deliberately excluded China, the second largest economy in the world, from participating. Meanwhile, the U.S. intended to use the new rules to address China's economic practices that it had long considered to be unfair and market-distortive, including trade, investment, IP, state-owned enterprises, competition regulation, and cross-border data flows.[599] Regarding the digital economy, top-level U.S. trade policymakers and negotiators were particularly concerned with China's efforts to enforce its concept of "cyber sovereignty".[600] Heavily lobbied by U.S. digital industry, the Obama administration decided to create binding and enforceable provisions on cross-border data flows in PTAs as a solution.[601] By incorporating the "Digital Dozen" principles into the model of new-generation trade agreements, the Obama administration believed TPP could address the China challenge, since, if approved, this agreement would cover around 40% of the global Internet users, and thus, can effectively set the rules for international data flows.[602]

---

[596] Negotiating countries may be concerned that their respective regional competitor states might trade greater concessions for accession in exchange for enhanced trade and investment flows, and hence, obtain a leg up against themselves in regional competition. This concern may prompt them to make concessions and enter the deal.
[597] Benvensti, *supra* (Democracy Captured), 58-59.
[598] Id.
[599] Mark Wu, *The "China Inc." Challenge to Global Trade Governance*, 57 HARV. INT'L L. J. 261, 314-320 (2016); Daniel Chow, *How the United States Uses the Trans-Pacific Partnership to Contain China in International Trade*, 17 CHIC. J. INT'L L. 370, 399-401 (2016).
[600] Aaronson and Leblond, *supra*, 255-256 (noting that China's concept of "cyber sovereignty" can be "defined as banning unwanted influence in a country's information space"); see e.g., USTR, *Fact Sheet: Key Barriers to Digital Trade*, March, 2016, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade (identifying China's arbitrary filtering and blocking of cross-border data flows as part of the key barriers to digital trade in the 2016 National Trade Estimate) [2016 USTR Fact Sheet].
[601] Azmeh and Foster, *supra*, 17; see e.g., 2016 USTR Fact Sheet (arguing that TPP contains thus far the most comprehensive rules to "combat restrictions on cross-border data flows, data localization requirements and other barriers to digital trade").
[602] Aaronson and Leblond, *supra*, 256. See Chow, *supra*, 384-387.

As such, TPP was negotiated on a "plurilateral-minus-one" basis, but somehow focused on the excluded one—China. If this strategy is achieved, China would be mired in a dilemma—either to join TPP on the terms largely set by the U.S. (along with its like-minded allies) to "correct" its economic practices, or risk being excluded from comprehensive trade and investment liberalization occurring in its neighboring region.[603] Through threats of trade and investment diversion, TPP could pressure China to liberalize its digital market and abandon its data restrictive measures targeted by the U.S. digital trade agenda.[604] Aimed at making advanced rules governing digital trade in the Asian-Pacific market and beyond, TPP therefore not only can serve as a model for future regional and multilateral rules, but also may function "as a tool to pressure China to accept what the Obama administration saw as the trade rules of the twenty-first century."[605]

(B) Evolution of Digital Trade Provisions from KORUS to TPP

Unlike traditional trade treaties, TPP formulated a high-standard set of digital trade provisions as a template for the future digital economy, dealing with regulatory issues relating to cross-border data flows, data localization, and data privacy protection. For our purposes, such a bold step of evolution in trade rulemaking is reflected in two major aspects below.

(a) Binding and Enforceable Commitments for Cross-Border Data Flows and against Data Localization

Before delving into the relevant provisions of TPP, it is worth noting that in 2007, Korea—US PTA (KORUS) was the first trade agreement with specific language to regulate cross-border data flows in its e-commerce chapter. Article 15.8 of the latter treaty provides that "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across border."[606] However, the aspirational language ("shall endeavor to refrain from…") does not strictly prohibit the use of illegitimate barriers to international data flows, which seemingly suggests the "soft law" nature of this provision. Nor does it define what constitutes "unnecessary barriers" or what does not (e.g., legitimate exceptions, if any).[607] Crafted in a manner as such, this provision appears non-actionable through international dispute settlement mechanism.[608]

These inadequacies are effectively remedied by TPP. As the first PTA to do so, TPP contains binding and enforceable commitments on free flows of data across borders, as well as a ban on data localization, reflecting the demands of key U.S. business interest groups.

---

[603] See Chow, *supra*, 370 (noting that "[i]f ratified, the TPP will be the largest mega free trade area in history and will encompass forty percent of world trade"); Aaronson, *supra (Digital Trade Imbalance)*, 10 (noting "TPP parties have a population of some 800 million people, or 11.4 percent of the world's total", and it "covers so many Internet providers and users").
[604] Azmeh and Foster, *supra*, 19.
[605] Id, 17.
[606] Korea-US PTA (KORUS), art. 15.8.
[607] Aaronson, *supra* (Digital Trade Imbalance), 8.
[608] Id., 8.

Two provisions are most relevant. Article 14.11 formulated a "hard" rule to require cross-border free data flows by default: "[e]ach Party shall allow the cross-border transfer of information by electronic means, *including personal information*, when this activity is for the conduct of the business of a covered person."[609] In parallel, article 14.13 provided that "[n]o Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[610]

First, the scope of these *horizontal* provisions is broad and comprehensive, making for robust protections of cross-border data flows across various economic sectors (except for financial services).[611] Under article 14.11, the guarantee of cross-border data transfers protects against both *de jure* and *de facto* data localization requirements. Unlike *de jure* localization measures that directly impose local processing and storage requirements, *de facto* localization measures incentivize foreign firms to store and process data collected within a state by implementing stringent data transfer restrictions.[612] A typical case in point in the latter's category may be the EU's General Data Protection Regulation (GDPR). By imposing restrictive conditions on cross-border personal data transfers for data privacy protection purposes, GDPR makes such transfers rather costly, risky, and burdensome in general.[613] By default, article 14.11 applies to both forms of localization measures, creating comprehensive protections for cross-border data flows.

In addition, article 14.13 prohibits a specific type of *de jure* localization requirements: "computer localization" measures that oblige foreign firms to "use or locate computing facilities" within its border "as a condition for conducting business" there.[614] This provision is largely tailored to address the growing concerns of cloud computing providers. Dominated by leading U.S. firms, this digital sector has strong commercial interests in creating a transnational digital infrastructure for data storage and processing, in order to maximize economic efficiency of their business model.[615]

Second, under articles 14.11 and 14.13, TPP creates legitimate public policy exceptions for states to restrict cross-border data flows or to localize computing facilities, but subjects such safety-valves to relatively stringent conditions.[616] To begin with, an impugned measure must not be "applied in a manner of arbitrary or unjustifiable discrimination or a disguised restriction on trade", reflecting the language of the chapeau clause under the GATT/GATS general exceptions.[617] In the context of the WTO, this condition requires "consistency of enforcement" in practice, such that a

[609] TPP, art. 14.13(2) (emphasis added).
[610] TPP, art. 14.13(2).
[611] TPP, art. 14.1 (the definition of a "covered person" does not include a "financial institution" or a "cross-border financial service supplier"). In the financial services chapter, TPP requires a member state to allow a covered financial institution to "transfer information in electronic or other form, into and out of its territory, for data processing" required in that institution's "ordinary course of business". Meanwhile, TPP member states retain the right to take measures to protect data privacy, or to require a financial institution to obtain prior authorization for prudential considerations. See TPP, chapter 11, Annex 11-B, Section B.
[612] Streinz, *supra* (Megaregulation), 332.
[613] *Id*. See eg. GDPR, arts. 44-47.
[614] TPP, art. 14.13(2).
[615] Streinz, *supra* (Megaregulation), 333.
[616] TPP, arts. 14.11(3), 14.13(3).
[617] TPP, arts. 14.11(3)(a), 14.13(3)(a). See GATT, art. XX; GATS, art. XIV.

respondent state can prove that the measure is not disguised protectionism or favoritism.[618] For instance, a member state shall not "single out one state or another for tougher application of extraterritorial provisions found in its data privacy law".[619] Neither can it maintain exceptions to its disputed measures for particular countries (but not others), or establish standards that "are not applied consistently to each country from day to day".[620]

To invoke these exceptions, the disputed measure also must be "necessary", requiring no restrictions on data transfers (or the location or use of computing facilities) "greater than are required to achieve the objective."[621] Under the WTO general exceptions (on which these clauses are largely based), the finding of necessity hinges on the existence of a "reasonably available" alternative that is less trade restrictive but achieves the same policy goal.[622] In WTO adjudication, this determination generally requires a holistic "weighing and balancing" of various factors, including the importance of the objective, the contribution of the measure to that goal, and its trade-restrictiveness.[623]

While protection of data privacy or cybersecurity is generally seen to qualify as "legitimate public policy objectives" here,[624] many of today's data privacy and cybersecurity measures might not justify their legitimacy under these TPP exceptions, if applying a stringent standard of review. Take the EU's data protection law for example, many leading privacy scholars argue that this regulatory measure might have exceeded the bounds of the GATS privacy exception.[625] This is because that the EU may not have consistently reached the "adequacy" decisions about the recipient countries' levels of data protection, making it difficult to meet the required "consistency of enforcement" condition.[626] In fact, when judging the permissibility of international personal data transfers to a non-EU jurisdiction, the EU seems to have, in part, used political criteria, rather than the objective factors as required under the GATS exceptions.[627] With respect to the necessity requirement, as found by Mira Burri, "[i]t can well be maintained that there are less trade restrictive measures that are reasonably available for achieving the EU's desired level of data protection." [628] If international adjudicators found this to be the case, the EU's data privacy laws would fail this relatively stringent test, and thus constitute disguised protectionism under GATS.[629] Recall that these "public policy objective" exceptions incorporate articles XIV(a), (b), and (c) of GATS,

[618] ROLF H. WEBER & DOMINIC STAIGER, TRANSATLANTIC DATA PROTECTION IN PRACTICE 58 (2017); Mitchell and Hepburn, *supra*, 205. Chander and Schwartz, *supra*, 9.
[619] Chander and Schwartz, *supra*, 9.
[620] Mitchell and Hepburn, *supra*, 205.
[621] TPP, arts. 14.11(3)(b), 14.13(3)(b).
[622] Appellate Body Report, U.S.-Gambling, WT/DS285/AB/R (April 7, 2005), paras. 304-305.
[623] Mitchell and Hepburn, *supra*, 203 (noting that generally, "[t]he more a measure contributes to its objective, the more trade-restrictiveness is likely to be tolerated", and vice versa).
[624] Yakovleva, *supra* (*Privacy Protection(ism)*), 491; Mitchell and Hepburn, *supra*, 209 (noting that while the term "legitimate public policy objective" in these clauses is undefined, since articles 14.11 and 14.13 incorporated GATS art XIV(a), (b), and (c), *mutatis mutandis*, reference to GATS art. XIV (including privacy, consumer protection, public order, public morals) may suggest that these policy goals qualify as such).
[625] See Chander and Schwartz, *supra*, 9.
[626] Kristina Irion, Svetlana Yakovlev & Marija Bartl, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements*, UNIVERSITY OF AMSTERDAM INSTITUTE FOR INFORMATION LAW (July 2016), at 55, https://www.ivir.nl/publicaties/download/trade_and_privacy.pdf.
[627] KUNER, *supra*, 66. Chander and Schwartz, *supra*, 10.
[628] Mira Burri, *Interfacing Privacy and Trade*, 53 CASE W. RES. J. INT'L L. 35, 66 (2021).
[629] *Id.*

mutatis mutandis. The strong resemblance of the structure and text may lead international adjudicators to refer to the relatively well-established WTO jurisprudence on these provisions for analytical guidance, finding EU data protection law unable to satisfy these TPP exceptions.

Third, TPP's protections for free data flows and against data localization are implemented by strong enforcement mechanisms. Unlike the KORUS whose provision on cross-border data flows is not actionable, these TPP commitments are enforceable through mandatory state-state dispute settlement mechanism, backed up by retaliatory trade sanctions to ensure compliance.[630]

Moreover, a covered investor or investment may also invoke substantive investment protection obligations in the investment chapter to challenge measures restricting data flows through investor-state dispute settlement mechanism.[631] To adjudicate such investor-state arbitration claims, investment tribunals should apply the relevant investment protective guarantees (such as expropriation, fair and equitable treatment, non-discriminatory treatment), rather than articles 14.11 and 14.13.[632] This means that while a host state can invoke the "legitimate public policy objectives" exceptions in chapter 14 in state-state proceedings, the same measures can still be challenged under substantive investment protective standards in investor-state arbitrations. Further, through nationality planning and regulatory arbitrage, multinational firms may invoke these investment guarantees even when their home jurisdiction is not or no longer a TPP member.[633]

In addition, TPP does not confer a state-state tribunal an exclusive jurisdiction to hear all disputes arising from alleged breaches of the e-commerce chapter.[634] Technically, its state-state dispute settlement mechanism may not preclude unilateral trade sanctions imposed by a complaining state. While the legal relationship between state-state proceedings under TPP and unilateral trade sanctions under domestic trade law is unclear, a complaining state may sidestep the former and invoke the latter to enforce articles 14.11 and 14.13. Though untested, this means of enforcement is not without precedent, as the Trump administration had invoked section 301 action to impose substantial tariffs on China for its alleged unfair, discriminatory, and burdensome trade practices (particularly with respect to IP protection).[635] Also, in 2017, the USTR published the National Trade Estimate Report on foreign trade barriers, adding foreign data localization measures as an important digital trade barrier under the "Special 301" watch list.[636] This means that if there is sufficient political willingness, the U.S. may deploy its domestic trade law tools—most notably, section 301 and/or special 301 actions—to protect free flows of data and sanction foreign data localization measures. Particularly, given that a member state can misuse or abuse TPP's self-judging "essential security interest" exceptions to justify data localization measures for thinly veiled protectionist purposes,[637]

---

[630] TPP, arts. 28.3, 28.20.
[631] TPP, arts. 14.2(4), 9.19.
[632] TPP, art. 9.19.
[633] Thomas Streinz, *Designing international Economic Data Law*, 115 ASIL PROCEEDINGS 73, 75 (2021).
[634] See TPP, chapter 28.
[635] See Kathleen Claussen, *Forgotten Statutes: Trade Law's Domestic (Re)turn*, 113 AJIL Unbound 40, 42-43 (2019) (noting that "the USTR has taken the position that Section 301 remains an available tool despite WTO rules and processes—a view it has asserted since the creation of the WTO"). This position may extend to the TPP rules and processes.
[636] USTR, *2017 National Trade Estimate Report on Foreign Trade Barriers*, at 3, 90, https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf.
[637] TPP, art. 29.2.

this means of enforcement may discipline and deter such acts of non-compliance through heavy sanctions, reserving these arguments for extraordinary security emergencies.

Collectively, this triple-barreled approach to enforcement may subject a non-compliant state to both trade sanctions and investor-state monetary damages, constraining the latter's regulatory autonomy to depart from the default rules of free data flows.

(b) Consumers' Data Privacy Protection

Another innovation of TPP is its provisions on data privacy protection, but this improvement is much more qualified, compared to the cross-border data transfer commitments. On the one hand, TPP has created stronger data privacy protection obligations than KORUS, since it requires states to adopt or maintain consumer protection laws and a legal framework to protect the personal information of e-commerce users.[638] On the other hand, TPP requires only a permissive privacy floor, without examining the merits of domestic data privacy systems. Rather, the existence of such a legal framework would suffice TPP's obligations. For that purpose, member states may take different approaches to protecting personal data, whether through comprehensive data privacy laws, sector-specific privacy laws, or laws providing for the enforcement of voluntary privacy commitments by private firms.[639] This permissive approach to data privacy protection is starkly different from TPP's approach to free data flows and data localization, as the latter subjects domestic data privacy measures restricting data transfers to relatively strict disciplines.

This stance demonstrates a prominent feature of the U.S. model of cross-border data transfer regulation in PTAs: establishing the "primacy of trade over privacy" by default.[640] While seeking to protect data privacy, individuals' informational privacy is conceptually framed as a matter of consumer protection, squarely anchored in the digital marketplace.[641] In this way, TPP redefines data privacy as instrumental "tools of international trade", manifesting an economic approach to protecting personal data.[642] Rather than human rights with intrinsic values, data privacy under these TPP provisions is normalized as an ancillary, subordinated value, playing an instrumental role to build trust in e-commerce and facilitate global economic flows.[643]

Essentially, this approach to data privacy reflects, and seeks to safeguard the U.S.' domestic information privacy law. While the EU protects individuals' rights to data protection and privacy as fundamental rights, the U.S. approach treats individuals' online privacy as a consumer right in the marketplace.[644] Also, an outlier in national legal system for data privacy, the U.S. takes a

---

[638] TPP, arts. 14.7(2), 14.8(2). Compare with KORUS, art. 15.5 (merely recognizing the importance of "transparent and effective measures to protect consumers" and regulatory cooperation to enhance consumer welfare).
[639] TPP, art. 14.8(2)(fn6).
[640] Chander and Schwartz, *supra*, 26-27.
[641] Id., 27.
[642] Yakoleva, *supra* (Privacy Protection(ism)), 492. Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"?*, 17 WORLD TRADE REV. 477, 484-487 (2018) (comparing an instrumental or economic approach to data privacy protection with a human rights approach that protects personal data and privacy as intrinsic values) ["Should Fundamental Rights"].
[643] Yakovleva, *supra* (Should Fundamental Rights), 484-485.
[644] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Privacy Law*, 106 GEO. L.J. 115, 132-37, 147-49 (2017); Yakoleva, *supra* (Privacy Protection(ism)), 492.

sectoral, patchwork approach to protecting information privacy, relying on a mix of narrowly targeted, sector-specific laws and regulations as well as business self-regulation.[645] This explains why the U.S. aims to ensure that different countries can develop different national approaches to data privacy protection in TPP, rather than to globalize data privacy standards.[646]

Finally, recognizant that divergent national data privacy systems can create trade barriers and increase compliance costs for digital firms, TPP points to some preliminary solutions. In addition to requiring states to publish information on their domestic personal data protection laws, TPP encourages members to develop "mechanisms to promote compatibility between these different regimes".[647] This provision intends to help TPP parties to find common ground between different data privacy systems, in efforts to remove barriers to data flows arising from divergent national regulations.[648] However, TPP stops short at proposing a specific mechanism to promote "compatibility" as such.

(C) TTIP and TiSA

In parallel to the TPP negotiations, the U.S. also negotiated new trade rules governing cross-border data flows at two other major plurilateral and regional venues, in order to incorporate the Digital Dozen principles.[649] These are the negotiations of TTIP with the EU and the Trade in Services Agreement (TiSA) with 22 most advanced economies (including the EU).[650] Specifically, the USTR vigorously pushed for the inclusion of binding, horizontal provisions on free data flows into TTIP and TiSA.[651] However, unlike TPP, such negotiations turned out to be far more difficult, due to strong opposition from numerous European countries.[652]

In these negotiations, European policymakers, civil society, and activists were very concerned that such a trade treaty would undermine the EU's commitments to protecting European citizens' personal data and privacy as fundamental rights.[653] Such concerns culminated after the Snowden revelations, exposing that many U.S. firms were sharing personal data of EU citizens with the U.S. government for national security purposes.[654] In addition, the EU's reluctance to sign up to the U.S.-designed data transfer provisions was partly due to the economic and strategic concerns that the European consumer market and digital economy may be dominated by leading American

---

[645] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STANFORD L. REV. 1315, 1331 (1999).
[646] Chander and Schwartz, *supra*, 27.
[647] TPP, art. 14.8(4)-(5).
[648] Aaronson, *supra* (Digital Trade Imbalance), 10.
[649] *Id*., 9.
[650] *Id*., 16.
[651] See Gaël Le Roux, *TTIP Negotiations, Policy Convergence, and the Transatlantic Digital Economy*, 19 BUS. & POL. 709, 731 (2017). Trade in Services Agreement (TiSA) Annex on Electronic Commerce, Wikileaks (2016), arts. 2, 9 (bracketed), https://wikileaks.org/tisa/ecommerce/TiSA%20Annex%20on%20Electronic%20Commerce.pdf.
[652] Azmeh and Foster, *supra*, 17.
[653] Aaronson, *supra* (Digital Trade Imbalance), 12, 16-17. James Fontanella-Khan, *Data Protection Ruled out of EU-US Trade Talks,* FINANCIAL TIMES (Nov. 5, 2013), https://www.ft.com/content/92a14dd2-44b9-11e3-a751-00144feabdc0.
[654] Aaronson, *supra* (Digital Trade Imbalance), 14.

digital firms under such terms.[655] As a result, provisions on cross-border data flows, and particularly, the exceptions thereof for data privacy purposes, became a highly contentious point (if not a deal breaker) in the TTIP and TiSA negotiations, featuring a divide between the U.S. and the EU.[656] As of today, both negotiations halted, and no agreements have been reached.

C. USMCA, and Subsequent PTAs

(A) USMCA

In 2019, the Trump administration's decision to withdraw from TPP created considerable inconsistency in U.S. digital trade policy, marking a major setback for the progress on the digital trade agenda.[657] After the U.S.' exit, however, the remaining 11 countries resurrected the deal as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), incorporating TPP's data governance provisions without substantial modifications.[658]

Moreover, during the Trump administration, the USTR expressed concerns with China's protectionist measures in the data-driven sectors, and showed the political willingness to respond with domestic trade tools.[659] During the early days of the Trump administration, numerous digital firms and industry associations mobilized to press for new rules governing digital trade and countering digital protectionism.[660] Many of such demands were incorporated in the U.S.-Mexico-Canada (USMCA) agreement (the revised NAFTA), which not only adopted most provisions of TPP's e-commerce chapter but also included some new features to further enhance its commitments.[661]

(a) Stronger Commitments on Transborder Data Flows

While retaining much of TPP's data transfer provisions, USMCA introduces several changes to strengthen the commitments for free data flows and against data localization. First, USMCA adopted TPP's provision against computer localization, but removed the public policy objective exceptions.[662] This modification sharpens this rule by substantially restricting states' regulatory autonomy to depart from this default setting.

Second, in article 19.11, USMCA incorporated TPP's article 14.11 to establish the default rule of free data flows across borders, but added a footnote to explain the "necessity" condition under the

---

[655] Azmeh and Foster, *supra*, 17-18.
[656] Yakoleva, *supra* (Privacy Protection(ism)), 493 (noting that the EU takes "a more cautious approach to cross-border data flows in trying to defend its regulatory autonomy to protect the fundamental rights to privacy and personal data", and that thus far, EU's PTAs contained no binding provisions on cross-border data flows).
[657] Azmeh and Foster, *supra*, 18.
[658] Streinz, *supra* (Megaregulation), 313. See CPTPP, Chapter 14 (E-Commerce).
[659] Office of the United States Trade Representative (USTR), *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974* (Washington, DC: USTR, 2018), https://goo.gl/ifbZ8n.
[660] Azmeh and Foster, *supra*, 18.
[661] *Id*. See USMCA, Chapter 19 (Digital Trade).
[662] USMCA, art. 19.12; compare with TPP, art. 14.12.

"legitimate public policy" exceptions.[663] It clarified that a domestic measure cannot invoke such exceptions, where "it accords different treatment to data transfers solely on the basis that they are cross-border in a matter that modifies the conditions of competition to the detriment of service suppliers of another Party."[664] Consistent with the prevailing interpretation of the necessity test under the WTO general exceptions, this clarification emphasizes the objective nature of this test, which does not recognize the regulatory intent of the state as a relevant factor in the assessment.[665] Rather, adjudicators should review the objective economic impact of the measure on the competition conditions of foreign service suppliers. Also, this footnote rejects the presumption that *international* transfers of data, in and of themselves, create greater risks to the legitimate public policy objectives than *domestic* data flows. Instead, the respondent state should show how its policy goals are compromised with concrete evidence.

Third, in the personal information protection provision, USMCA adds a recognition that "any restrictions on cross-border flows of personal data are *necessary* and *proportionate* to the risks presented," despite the "importance of ensuring compliance with measures to protect personal information."[666] Focused on preventing regulatory overkill, this clause can provide the context to interpret the "necessity" condition under the public policy objective exceptions. As such, a state cannot adopt measures that are more restrictive on international data flows than what is necessary to achieve data privacy protection.

Finally, different from TPP, USMCA breaks new ground by extending the commitments against computer localization to the financial sector. As provided by article 17.18, no member state "shall require a covered (financial institution or cross-border financial service supplier) to use or locate computing facilities in (its) territory as a condition for conducting business" there.[667] That said, this obligation is subject to a qualification—the host state's financial regulatory authorities should, "for regulatory and supervisory purposes, have immediate, direct, complete, and ongoing access to information processed or stored on" those computing facilities outside its territory.[668] Aimed at narrowing the gap between transborder financial and non-financial personal data flows, this provision reflects the lobbying efforts by U.S. financial and banking sectors, whose business model relies on unhindered flows of personal data across borders.[669]

(b) Consumers' Data Privacy Protection

With respect to data privacy regulation, USMCA adopted TPP's provision on personal information protection, but added certain notable features. First, it referenced soft law instruments of the APEC Privacy Framework and OECD Guidelines (2013) as "principles and guidelines of relevant international bodies" that a state should consider when developing a domestic legal framework to protect personal data.[670] Second, it expressly recognizes the APEC Cross-Border Privacy Rules (CBPR) system as "a valid mechanism to facilitate cross-border information transfers while

[663] USMCA, art. 19.11; compare with TPP, art. 14.11.
[664] USMCA, art. 19.11(fn5).
[665] Yakoleva, *supra* (Privacy Protection(ism)), 491.
[666] USMCA, art. 19.8(3) (emphasis added).
[667] USMCA, art. 17.18(2). See id., art. 17.1.
[668] USMCA, art. 17.18(2).
[669] See Streinz, *supra* (Megaregulation), 331-32.
[670] USMCA, art. 19.8(2).

protecting personal information."[671] Collectively, these modifications have consolidated and refined TPP's economic approach to data privacy protection.

(1) An Economic Approach to Data Privacy Protection

The OECD Guidelines and APEC Framework manifest an economically driven, instrumental approach to data privacy protection, as opposed to the EU's human rights approach.[672] While privacy concerns are present in these instruments, the economic rationale is predominant. Substantively, these instruments establish a lower set of data privacy standards than European data privacy law.

An updated version of the 1980 Guidelines, the 2013 OECD Guidelines retain the dominant economic rationale underlying its predecessor, primarily focused on promoting cross-border personal data flows and minimizing regulatory restrictions thereon.[673] On data privacy protection, the OECD Guidelines (2013) incorporate the eight core principles of the original Guidelines, which were written at a high level and were not prescriptive enough.[674]

Similarly, the APEC Privacy Framework, largely modeled on the OECD Guidelines, is "a voluntary set of standards designed to protect personal data transferred outside the APEC member States by use of the principle of 'accountability'."[675] As stated in its preamble, this Framework, while reaffirming the value of individuals' data privacy, "aims at promoting electronic commerce."[676] In contrast, data privacy protection is essentially conceptualized as an instrumental tool to address domestic regulations that may unnecessarily restrict cross-border data flows, as well as a necessity to bolster consumer confidence and prosper digital trade, rather than intrinsic values of human rights.[677]

Though consistent with the core principles of the OECD Guidelines, the data privacy standards under the Framework are generally lower than those under European data privacy law, and come "with a mild prescriptive bite".[678] A principles-based model, the Framework also leaves member economies considerable flexibility to implement it in a way that reflects their social, economic, legal, and cultural differences.[679] Rather than prescribing how it should be implemented in a specific way, numerous implementation methods may be proper, ranging from legislation to business self-regulation.[680] This means that divergence may persist among member economies that have implemented the Framework.[681] Finally, many principles of the Framework are subject to

[671] USMCA, art. 19.8(6).
[672] Yakovleva, *supra* (Should Fundamental Rights), 484-85.
[673] BYGRAVE, *supra*, 44 ("According to Michael Kirby, who headed the Expert Group responsible for drafting the original Guidelines, the OECD's work in the field was motivated primarily by economic concerns"); Id., 484.
[674] OECD Guidelines 2013, paras. 7-14.
[675] KUNER, *supra*, 50. See APEC, APEC Privacy Framework 2015, https://www.apec.org/publications/2017/08/apec-privacy-framework-(2015), para. 9 [APEC Privacy Framework].
[676] APEC Privacy Framework, Preamble, para. 5. See id., para. 1. See BYGRAVE, *supra*, 75-76.
[677] BYGRAVE, *supra*, 76. See APEC Privacy Framework, paras. 1-4.
[678] BYGRAVE, *supra*, 76. KUNER, *supra*, 51 ("The lack of binding effect and the divergence of the Framework from principles of EU data protection law have led to accusations that the level of protection under it is too low").
[679] KUNER, *supra*, 51. APEC Privacy Framework, para. 17.
[680] BYGRAVE, *supra*, 76; see APEC Privacy Framework, paras. 37-38.
[681] KUNER, *supra*, 51.

extensive derogations, which are permitted under laxer criteria than under European data privacy law.[682]

Second, aligned with USMCA's provisions on cross-border data flows, the OECD Guidelines and APEC Framework establish the default rules of transborder free flows of personal data, and primarily rely on the accountability principle to protect data privacy.

In this regard, the OECD Guidelines generally permit international transfers of personal data, but give national regulators discretionary powers to restrict or block data flows in limited circumstances.[683] Under the 2013 Guidelines, a member state "should *refrain from restricting* transborder flows of personal data", where (a) the *recipient country* "substantially observes these Guidelines" or (b) the *data controller* maintains "sufficient safeguards" (including "effective enforcement mechanisms and appropriate measures") "to ensure a continuing level of protection *consistent with* these Guidelines."[684] Relatedly, these Guidelines require data controllers to remain accountable for personal data under their control, even when those data have crossed national borders.[685]

Likewise, the APEC Privacy Framework does not expressly permit member states to restrict or ban cross-border personal data flows to jurisdictions with insufficient levels of data privacy protection. Rather, it relies on the principle of "accountability" to protect consumers' data privacy.[686] At the core, the "accountability" principle makes the original data collectors accountable for ensuring compliance with the Framework, regardless of the recipients' locations.[687] Specifically, this principle requires data controllers to obtain the consent of the individual whose data are to be transferred, or to "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."[688] In this way, the Framework adopts an organization-based approach to regulating data privacy, placing the duties of data privacy protection on individual firms that control "the collection, holding, processing, use, disclosure or transfer of personal information" (i.e., data controllers).[689]

(2) Promoting a U.S. Model of Accountability Mechanism[690]—the APEC CBPR System

Unlike TPP that remains silent on this matter, USMCA expressly recognizes the APEC CBPR as a sufficient mechanism to protect information privacy for cross-border flows of personal data. Established by the APEC in 2011, the CBPR system is a government-backed data privacy

[682] BYGRAVE, *supra*, 76; see APEC Privacy Framework, para. 18.
[683] KUNER, *supra*, 76.
[684] OECD Guidelines 2013, para. 17 (emphasis added).
[685] *Id.*, para. 16.
[686] APEC Privacy Framework 2015, paras. 32. Yakovleva, *supra* (Should Fundamental Rights), 485.
[687] KUNER, *supra*, 71.
[688] APEC Privacy Framework, para. 32. See BYGRAVE, *supra*, 77 (noting that the possible restriction on international personal data flows is broached under the accountability principle).
[689] See APEC Privacy Framework, para. 10.
[690] "Accountability mechanisms" refer to measures taken by firms to provide privacy protections for international data transfers, making them "accountable" for their processing of personal data. See Chander and Schwartz, *supra*, at 33, 35-36.

certification mechanism that companies (data controllers) can opt-in to demonstrate compliance with the data privacy standards of the APEC Privacy Framework.[691] Through CBPR, certified firms and governments of the participating economies work together to ensure that personal data flowing across borders would be protected by the privacy standards prescribed thereunder, and are legally enforceable across these jurisdictions.[692]

First, a participating economy must certify at a country level to ensure that the CBPR requirements are legally enforceable against certified companies.[693] While this country-level certification creates no binding obligations *per se* for any companies in its territory, it opens the door for the latter's voluntary participation in CBPR.[694] Second, a participating company should apply for certification from an independent, CBPR-recognized accountability agent.[695] The accountability agent can be a public or private sector body, and will be designated by each participating economy.[696] In the certification process, the accountability agent evaluates whether the applicant company's privacy policies and practices meet CBPR's data privacy standards, based on a list of fifty regulatory requirements provided thereunder.[697] If positive, the company would be certified as CBPR-compliant, and then will be listed in a publicly accessible directory.[698] Third, certified companies should implement privacy safeguards to protect personal data. Failing that, the accountability agents may investigate complaints from consumers and resolve disputes involved to ensure compliance.[699] Meanwhile, the privacy enforcement authority (PEA) of the participating economy can enforce the certification against a certified company.[700]

Designed to implement the APEC Privacy Framework, the CBPR system essentially imposes a minimum set of data privacy standards on certified data controllers, creating a voluntary opt-in mechanism overseen by the accountability agents and public authorities. In addition to its basic opt-in structure, the CBPR system allows third-party private organizations to oversee its compliance, characterized by a pro-self-regulation model of data privacy protection.[701]

Through the CBPR system, certified firms are entitled to transfer personal data to overseas certified recipients (whether a foreign affiliate or another company), without meeting additional regulatory requirements to protect data privacy.[702] For instance, CBPR-compliant U.S. firms can transfer

---

[691] APEC, *What is the Cross-Border Privacy Rules System*, October 2021, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015 ["*What is the Cross-Border Privacy Rules System*"]. Bygrave, *supra*, 78.
[692] *What is the Cross-Border Privacy Rules System*, *supra*.
[693] APEC, *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines*, November 2019, 8, https://www.privacy.gov.ph/wp-content/uploads/2021/10/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019-1.pdf ["APEC CBPR"].
[694] Chander and Schwartz, *supra*, 34.
[695] APEC CBPR, *supra*, 9.
[696] *Id.*, 8.
[697] *Id.*, 5, 9-10.
[698] *Id.*, 6.
[699] *Id.*, 6.
[700] *Id.*, 6, 10.
[701] See Paul Schwartz, *Global Data Privacy: The EU Way*, 94 NYU L. R. 771, 797 (2019) ["The EU Way"].
[702] Infocomm Media Development Authority, *APEC Cross Border Privacy Rules (CBPR) System*, October 30, 2019, https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification

personal data from certified Japanese companies to the U.S., without a decision from the Japanese government that U.S. data privacy law is adequate. Among participating economies of CBPR, a country cannot even restrict transfers of personal data by a CBPR-compliant company to a jurisdiction with a laxer privacy regime.[703] In this way, this mechanism seeks to bridge divergent national data privacy laws and build trust for consumers' online privacy protection, substantially reducing regulatory barriers to cross-border personal data flows for global trade.[704]

However, the CBPR system is subject to its own limitations. First, while CBPR can establish a privacy floor consistent with the APEC Privacy Framework, whether this level of data protection is sufficient is debatable. A "principles-based" model, the APEC Privacy Framework's data privacy standards are generally lower and less prescriptive than those of European data privacy law, and are subject to broad derogations under laxer criteria.[705] Thus, the level of data privacy protection provided by CBPR is seen to be weaker than that of the GDPR.[706] For example, unlike the GDPR, the CBPR system applies only to data controllers (not data processors), does not create affirmative rights to consumers, imposes laxer conditions for cross-border personal data transfers, and does not require notification for data breaches.[707]

It remains to be seen how many companies will join this system. So far, the CBPR system seems to be underperforming. From its inception in 2011 to January 2019, this mechanism has only 23 participating firms.[708] Finally, it is unclear how CBPR would be enforced in practice. In the U.S., the Federal Trade Commission (FTC) is the designated PEA. Thus far, its enforcement of CBPR seems to be rather rare in practice, compared with European data privacy authorities' vigorous enforcement of EU data privacy law.[709]

Overall, the CBPR system is a concretization of the mechanisms to promote "compatibility" or "interoperability" between different national regulatory approaches to personal data protection, as referenced by TPP and USMCA.[710] While the precise meaning of "compatibility" or "interoperability" remains undefined, according to a leading commentator, this term suggests "a situation in which different data privacy regimes co-exist harmoniously and, as a result, permit personal data to flow between countries and organizations but without unduly compromising the privacy-related interests of the data subjects."[711] As such, U.S.-led initiatives to promote CBPR advances four important goals.

---

[703] Andrei Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (January 3, 2019), https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.
[704] *Id*. Chander and Schwartz, *supra*, 29.
[705] BYGRAVE, *supra*, 76. KUNER, *supra*, 51.
[706] See KUNER, *supra*, 72.
[707] Gribakov, *supra* (for cross-border personal data transfers, GDPR requires companies to obtain "explicit consent" from data subjects or have another legal basis, while CBPR permits data controllers to "exercise due diligence and take reasonable steps" as an alternative to obtaining consent, and it is unclear what legal standards (if any) should apply to determine "due diligence" or "reasonable steps", as CBPR is principles-based).
[708] *Id.*
[709] *Id.* ("In fact, during the CBPR's existence there is no evidence of a company losing its CBPR certification; the only enforcement actions taken by the FTC were against three companies falsely claiming to be CBPR certified").
[710] See TPP, art. 14.8(5); USMCA, art. 19.8(6).
[711] BYGRAVE, *supra*, 49.

First, rather than achieving the *uniformity* of national privacy laws, such efforts seek to ensure the regulatory autonomy of countries to maintain *different* data privacy regimes.[712] Indeed, the CBPR system by no means replaces or changes a participating economy's domestic laws and regulations, but is designed to provide an international minimum level of data privacy protection, in order to facilitate cross-border personal data flows.[713] This accommodates the U.S.' needs to safeguard its data privacy approach from being challenged.

Second, this model of data governance not only builds on, but also seeks to export the U.S.' domestic approach to data privacy protection to its trading partners. Under the U.S.' sectoral, piecemeal approach, business self-regulation has long been playing an indispensable role in setting the standards of individuals' information privacy.[714] Given that leading U.S. digital and service firms have thrived under this regulatory approach,[715] promoting this model as an international approach (over the EU's GDPR) would well serve U.S. interests.

Third, by promoting CBPR as a valid mechanism for cross-border personal data flows, the U.S. not only could lower the transaction costs and smooth the process for businesses to transfer personal data across borders,[716] but also may indirectly raise the bar for permitted national restrictions on such transfers. Notably, the greater the international recognition of CBPR as a sufficient mechanism to regulate cross-border data exchange, the more likely that it is deemed "a reasonably available" alternative that can achieve data privacy protection but is less trade restrictive. This would make it difficult to justify more stringent national data flow restrictions as legitimate exceptions under the objective "necessity" and "proportionality" test stipulated by TPP and USMCA.

Fourth, compared with the EU's regulatory approach, the CBPR system establishes a lower threshold for cross-border personal data flows and provides a more business-friendly solution for data operators. As noted, governments of the participating economies under the CBPR would not examine whether a recipient jurisdiction ensures an "adequate" level of protection for personal data, as required by the GDPR.[717] Instead, they would treat certified companies as providing sufficient data privacy protection by default, unless otherwise proven. Further, application of the CBPR system would generally create lesser compliance costs and administrative burdens for data exporters, compared with the EU's accountability mechanisms (i.e., Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) that enable firms to transfer personal data outside Europe absent a country-level "adequacy" decision by the European Commission).[718] While the CBPR system is designed to enforce the relatively permissive principles of the APEC Privacy Framework, the SCCs and BCRs implement stringent data privacy standards modelled on EU data protection law, and are much more inflexible, burdensome, and time-consuming for companies to use.[719]

---

[712] Chander and Schwartz, *supra*, 28.
[713] APEC CBPR, *supra*, 11.
[714] Reidenberg, *supra*, 1331.
[715] Chander, *supra* (Silicon Valley), 648.
[716] Chander and Schwartz, *supra*, 34 (noting that the CBPR creates "a formulation that lowers transaction costs for organizations by providing pre-approved principles that would smooth the process of international data transfers.").
[717] GDPR, art. 45.
[718] See GDPR, arts. 46-47; EU Data Protection Directive 1995, art. 26(2).
[719] Chander and Schwartz, *supra*, 33-36; Schwartz, *supra* (The EU Way), 794.

These aspects explain why the U.S. has been promoting CBPR as a "model for global interoperability among privacy regimes", as well as a better approach to regulate cross-border personal data flows than the GDPR.[720] Indeed, given that numerous countries have increasingly adopted an EU-style data protection law (including the "adequacy" requirements for cross-border personal data transfers),[721] the strategic window for the U.S. to promote its preferred regulatory model is gradually closing.[722] Thus far, nine economies have joined the CBPR system, including the U.S., Canada, Mexico, Japan, South Korea, Singapore, Australia, the Philippines, and Chinese Taipei.[723] And Japan's amended privacy law recognizes CBPR as a valid mechanism for transferring personal data across borders.[724] In April 2022, the U.S. has started an initiative to create a Global Cross-Border Privacy Rules Forum, aimed to establish a Global CBPR system to facilitate and promote international personal data transfers.[725] If successful, such efforts may "establish an international certification system based on the APEC CBPR", upgrading CBPR from a regional accountability mechanism to a global one.[726]

(B) Subsequent Trade Negotiations

After the USMCA, the Trump administration has successfully negotiated the U.S.-Japan Digital Trade agreement. Paralleling the USMCA, this treaty likewise seeks to create comprehensive and high-standard digital trade rules to address digital trade barriers, support various digitally-enabled suppliers, and set the standards for other trade agreements to emulate.[727] To put this agreement in context, it bears noting that just a few months preceding its conclusion, Japanese Prime Minister Shinzo Abe presented the notion of "Data Free Flow with Trust" in the 2019 G20 Osaka summit, which made into the G20 Osaka Leaders' Declaration.[728] Though vague in its meaning, this concept emphasizes the commitments to facilitating cross-border free data flows, the needs to strengthen consumer and business trust through data privacy protection, as well as the importance

---

[720] APEC, *APEC Cross-Border Privacy Rules System Goes Public*, NEWS RELEASE (July 31, 2012), https://www.apec.org/Press/News-Releases/2012/0731_cbpr (U.S. Federal Trade Commissioner Edith Ramirez: "We hope that many more APEC economies will soon join and help realize the system's potential as a model for global interoperability among privacy regimes."); see Clare Sullivan, *EU GDPR or APEC CBPR?,* 35 COMPUTER LAW AND SECURITY REVIEW 380, 381 (2019).

[721] Chander and Schwartz, *supra*, 17, 19.

[722] Gribakov, *supra*.

[723] Government, *Cross Border Privacy Rules System*, April 15, 2022, http://cbprs.org/government/.

[724] Gribakov, *supra*.

[725] U.S. Department of Commerce, *Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum*, https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border; see U.S. Department of Commerce, *Global Cross-Border Privacy Rules Declaration*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[726] U.S. Department of Commerce, *Global Cross-Border Privacy Rules Declaration FAQ*, https://www.commerce.gov/sites/default/files/2022-04/Global-Cross-Border-Privacy-Rules-Declaration-FAQ.pdf.

[727] USTR, *Fact Sheet on US-Japan Digital Trade Agreement*, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement.

[728] Ministry of Foreign Affairs of Japan, *A Summary of the G20 Osaka Summit*, June 29, 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/overview/; G20 Osaka Leaders' Declaration, para. 11, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.

of promoting interoperability among different legal frameworks.[729] While "trust" requires an evaluation on whether the legal protection of data privacy in the recipient country is sufficient, this notion cautions against "the risks of overregulation and inter-regime conflicts", which would make data protection overly burdensome, and hence, will unnecessarily undermine digital trade.[730] Overall, "data free flow with trust" thus strikes a balance in favor of "data free flow", and frames data privacy protection as an instrumental tool to build trust in e-commerce and facilitate digital trade. The U.S. and Japan closely aligned in endorsing "data free flow with trust", and signed the Digital Trade agreement shortly after the Osaka G20 Summit in 2019.[731]

This treaty has adopted USMCA's provisions on free data flows, data localization, and personal data protection without much modification.[732] Like the USMCA, the U.S.-Japan Digital Trade agreement extended the rules against data localization to the financial sector, provided that the relevant financial regulators have access to those data necessary to fulfill their regulatory and supervisory mandate.[733] Yet, as a standalone digital trade agreement, this pact is not backed up by state-state or investor-state dispute settlement mechanisms, raising questions about its enforceability.[734]

In the post-Trump era, the Biden administration, while indicating that it is not currently interested in joining CPTPP, has announced plans for reaching a digital trade agreement with Indo-Pacific economies.[735] As part of an Indo-Pacific Economic Framework, this agreement may follow the template of the U.S.-Japan Digital Trade agreement.[736] In this way, such a U.S.-led regional digital trade agreement can set standards for the digital economy and data governance, and counter China's more active engagement in regional trade negotiations in pursuit of different policy priorities.[737]

Finally, during the plurilateral negotiations of the WTO Joint Statement Initiative (JSI) on E-commerce, the U.S. submissions on the proposed text of a digital trade agreement is primarily based on the data transfer provisions of the USMCA and U.S.-Japan Digital Trade agreement,[738] in efforts to export its small group consensus on data regulation to a much wider range of trade partners. However, despite the U.S.'s push for high-standard protection for free data flows, it might

[729] G20 Osaka Leaders' Declaration, para. 11.
[730] David G Litt and A Reid Monroe-Sheridan, *The US-Japan Digital Trade Agreement and "Data Free Flow with Trust"*, USALI (February 3, 2022), https://usali.org/usali-perspectives-blog/the-us-japan-digital-trade-agreement-and-data-free-flow-with-trust.
[731] *Id.*
[732] U.S.-Japan Digital Trade agreement, arts. 11, 12, 13, 15.
[733] *Id.*, art. 13.
[734] See *id.*
[735] Biden Administration Plans for an Indo-Pacific Economic Framework, CONGRESSIONAL RESEARCH SERVICE (February 25, 2022), https://crsreports.congress.gov/product/pdf/IN/IN11814.
[736] *Id.* Peter Martin et al., *Biden Team Weighs Digital Trade Deal to Counter China in Asia*, BLOOMBERG (July 13, 2021), https://www.bloomberg.com/news/articles/2021-07-12/biden-team-weighs-digital-trade-deal-to-counter-china-in-asia.
[737] Peter Martin et al., *supra*.
[738] *Digital Trade and U.S. Trade Policy*, CONGRESSIONAL RESEARCH SERVICE (December 9, 2021), at 43, https://sgp.fas.org/crs/misc/R44565.pdf.

be challenging to reach such an agreement, given various member states' divergent regulatory approaches on this contentious issue—particularly the differing preferences of the Big Three.[739]

V. POLICY DIFFUSION

At the international level, U.S.-promoted data transfer provisions (including those on cross-border data flows and data localization) have been increasingly diffusing among other follower countries, influencing a growing number of foreign governments' trade policymaking. Broadly speaking, the spread of U.S.-designed norms consists of two different scenarios.

In the first scenario, the norm diffusion is a natural and autonomous outcome of U.S.-led trade lawmaking initiatives. By deploying forum-shifting to advance its preferred digital trade rules, the U.S. was able to conclude PTAs with trade partner countries on its desired terms, making these foreign governments sign up to U.S.-promoted data transfer provisions.

In this process, the competitive lawmaking strategy of vertical forum-shifting is often instrumental in diffusing U.S.-designed digital trade rules internationally. By negotiating bilateral, plurilateral, and regional PTAs below the multilateral level, the U.S. managed to divide and fragment its trade partners, amplify its market clout and bargaining leverage against foreign negotiators, and exploit their economic dependencies and vulnerabilities.[740] Meanwhile, since the U.S. conditions its market access and preferential trade liberalization on the conclusion of a PTA, such issue-linkage may pressure or incentivize foreign trade partners with differing preferences to make concessions on some sensitive matters (such as data flows),[741] thus altering their cost-benefit analyses. For countries that compete with each other and which share similar market characteristics, U.S.-led PTA negotiations may create a competitive environment for them to join the deal, in order to maintain an advantage in regional economic competition.

As such, through forum-shifting, the U.S. was able to export U.S.-designed data transfer provisions through new-generation PTAs, causing other treaty parties to internalize its preference in their trade policymaking. As a result, today, U.S. trade partners that hope to strike a digital trade agreement (or chapter) with the U.S. typically need to accept the USMCA's digital trade rules as a baseline position—including commitments to unrestricted data flows, prohibition against data localization, and the acceptance of the APEC CBPR system to protect data in transit.

In the second scenario, many third countries are increasingly embracing the U.S. template of digital trade rules in their own PTAs, even in the absence of the U.S. as a trade negating partner.

---

[739] *Id.*, 44 (noting that "the EU's strict rules on data privacy impose more constraints on cross-border data flows compared with U.S. laws, making it unclear if the two sides will be able to reconcile their different regulatory approaches to create common rules", and that "with regard to data flows and data storage, China has proposed the negotiations to be limited to exploratory discussions rather than establishing obligations and has generally supported non-binding standards").

[740] See *infra* section IV.B.(A) (describing the U.S.'s negotiating tactics of "strategic fragmentation" and "divide and conquer").

[741] *Id.*

Widely regarded as the "gold standards" for future global digital trade,[742] U.S.-designed data transfer provisions have been increasingly adopted in subsequent PTAs by U.S. trade partners and beyond, even when the U.S. is off the negotiating table. As noted earlier, though the U.S. withdrew from TPP, the remaining 11 Asian-Pacific negotiating partners essentially incorporated its data transfer provisions into CPTPP. Other PTAs—particularly, those concluded by Latin American countries—have closely followed these provisions as boilerplate clauses to regulate cross-border data flows. These treaties include 2016 Chile-Uruguay PTA, 2016 Singapore-Australia PTA, 2017 Argentina-Chile PTA, 2018 Australia-Peru PTA, 2020 Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore.[743]

Meanwhile, at the plurilateral WTO JSI negotiations on e-commerce, countries such as Canada, South Korea, Japan, the U.K., and Singapore have emulated such provisions in their submissions for a proposed digital trade agreement.[744]

This scenario of policy diffusion suggests the strong willingness of third countries to converge to the U.S. regulatory approach—largely because they perceive such digital trade rules as the most "advanced" model,[745] reflecting their wish to spur digital trade flows and develop domestic digital industries.[746]

In both scenarios, four major mechanisms of policy diffusion are most relevant to explain the popularity of U.S.-designed digital trade rules. The first one is coercion: as noted earlier, in PTA negotiations, the U.S. strategically links the benefits of market access and trade liberalization to the adoption of its preferred rules, thus leveraging its economic power to compel and/or entice a foreign government to converge to its regulatory standards.[747] To be clear, the U.S. may find it difficult to coerce a rival economic power with a starkly different preference (such as the EU and China which prioritize privacy and national security, respectively) to accept its desired trade rules on data flows. Nevertheless, the U.S. is often adept at using its dominant economic power to impose its preference on smaller countries, especially those that are heavily reliant on its market access.

Second, some countries are inclined to imitate the digital trade policies of the U.S., as they perceive the latter as a "role model" and forerunner state in terms of developing the digital economy.[748] Given that the U.S. has a dominant digital industry, some follower countries may find it highly

---

[742] Streinz, *supra*, 341.
[743] 2016 Chile-Uruguay PTA, arts. 8.10-8.11; 2016 Singapore-Australia PTA (updated), arts. 23-24; 2017 Argentina-Chile PTA, arts. 11.6-11.7; 2018 Australia-Peru PTA, arts. 13.11-13.12; 2020 DEPA, arts. 4.3-4.4.
[744] WTO Electronic Commerce Negotiations, Consolidated Negotiating Text, December 14, 2020, INF/ECOM/62/Rev. 1, at 27-31.
[745] Streinz, *supra* (Megaregulation), 337-40 (noting the prevalence of the neo-liberal trade discourse (liberalized trade "lifts all boats") in global digital trade policymaking).
[746] Rodrigo Polanco, *Regulatory Convergence of Data Rules in Latin America*, in BIG DATA AND GLOBAL TRADE LAW 269-70 (Mira Burri ed., 2021).
[747] For a detailed discussion of the "coercion" mechanism, see Frank Dobbin, Beth A. Simmons, and Geoffrey Garrett, *The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning*, 33 ANNUAL REVIEW OF SOCIOLOGY 449, 454 (2007).
[748] For a detailed discussion of the "imitation" mechanism, see Cheng-Yun Tsang & Ping-Kuei Chen, *Understanding Policy Diffusion Mechanism of Financial Regulatory Innovation*, 30 ASIA PACIFIC LAW REVIEW 21, 30 (2022).

reputed in data governance.[749] Instead of comprehensively evaluating different policies or researching policy innovations, later-comer regulators may put trust in a widely recognized successful "role model", thus mimicking U.S.-promoted template as a regulatory shortcut to develop their own digital industries.

Third, the competition mechanism can also facilitate the policy diffusion process. When a direct competitor (such as a neighboring country) has followed U.S.-designed digital trade rules, peer pressure can lead a country sharing similar policy goals or market features to adopt the same policies, in order to establish a competitive advantage in the regional or global digital markets.[750]

Fourth, some developed countries may learn from the regulatory experiences of a leading digital economy (such as the U.S.), if they believe that its innovative rules are useful to address their similar policy concerns (e.g., removing foreign barriers to digital trade, minimizing transaction costs, and leveling the playing field for their export-oriented digital firms).[751]

These four major mechanisms are not mutually exclusive. Rather, some of them may function in combination to reinforce the incentives of a third country to follow U.S.-promoted norms. As noted earlier, the deployment of coercion is typically more relevant to explain how the U.S. pushed for its preferred rules before smaller countries with divergent preferences during international bargaining, though it cannot explain the second scenario of norm diffusion. Regarding the latter, it is often the "imitation" or "learning" mechanism that is animating the diffusion process, pushing and pulling foreign governments to accept U.S.-promoted data transfer provisions. Where the U.S. negotiates a PTA with a like-minded trade partner facing similar policy challenges or a follower country that has faith in its data governance model, the international bargaining may become much easier, as "learning" or "imitation" could come into play. Finally, whether the U.S. is present or not in trade negotiations, peer pressure (the "competition" mechanism) may also tilt the balance in favor of norm diffusion.

With a growing number of countries on board with its preferred governance model, the U.S. is empowered to establish its regulatory "sphere of influence", using U.S.-led PTAs to establish rules for the global digital economy and shape transnational data governance.

VI. CONCLUSION

Within the emerging transnational regime complex, the U.S. has been seeking to reposition the governance of cross-border personal data transfers to the international trade regime, subjecting domestic regulatory restrictions on such transfers to the scrutiny by the trade law disciplines. To that end, the U.S. has been deploying a lawmaking strategy of regime- and forum-shifting, pushing for its preferred rulemaking at the parallel venues of the WTO and PTAs.

Initially, the focus of the U.S.' efforts was centered on the multilateral forum of WTO. Through *horizontal regime shifting*, the U.S., along with its like-minded allies, created a multilateral trade agreement to govern trade in services, achieving some success in extending the reach of

[749] See *id.*
[750] For a detailed discussion of the "competition" mechanism, see *id*., 28-29.
[751] For a detailed discussion of the "learning" mechanism, see *id*., 29-30.

international trade law to cross-border data flows. Largely reflecting the demands of U.S. financial sector, GATS contains binding and disputable rules that can be invoked to challenge domestic measures restricting transborder data flows. However, formulated in a pre-Internet era, this agreement is subject to its inherent limitations—including its outdated classifications, member states' sectoral commitments, and the difficulty in handling related policy challenges—generating substantial legal uncertainties. As a result, GATS is not sufficiently adaptable to the data-driven economy and technologies not envisioned by its rules, evincing the "problem of interpretative 'technological translation'".[752]

Afterwards, despite U.S.-led initiatives to achieve comprehensive and deeper liberalization of digital trade, multilateral trade negotiations stalled without making substantial headway. Developing countries and emerging markets, exemplified by the African Group, used the WTO forum to build a powerful coalition to oppose such efforts. Leveraging the one-country-one-vote decision-making rule, these countries have successfully blocked the making of new digital trade rules on the terms of the U.S. Further, U.S.-promoted efforts to update and reform the WTO's digital trade rules were undermined by the lack of a strong coalition among developed countries, especially between the U.S. and the EU (given their stark regulatory divergence on cross-border personal data transfers). This stalemate of WTO negotiations has led the U.S. to pursue *vertical forum-shifting* through bilateral, plurilateral, and regional rulemaking below the multilateral level.

Through new-generation PTAs, the U.S. strives to transpose the Digital Dozen principles into international trade rules, setting the standards for digital trade and global economic governance. Reflecting U.S. digital trade agenda, these rules include binding and enforceable commitments for free data flows and against data localization, provisions setting a permissive floor of data privacy protection to facilitate digital trade, and the recognition that a U.S.-promoted accountability mechanism (CBPR) serves as a valid system to protect information privacy for international data transfers. At the core, these legal and policy prescriptions seek to establish the default rules of unrestricted data flows cross borders, to require national regulations restricting such flows to be justified as legitimate exceptions, and to maintain national regulatory autonomy to adopt different data privacy frameworks. Meanwhile, the U.S. strives to promote an economic approach to data privacy protection as an institutional alternative to the GDPR, shifting the focus of data privacy governance from prescriptive governmental regulations to business self-regulation.

Through vertical forum-shifting, the U.S. could magnify and better leverage its asymmetrical economic power to make international rules based on its preferences and interests. In so doing, the U.S. can divide and fragment its trade partners, play into their economic dependencies and vulnerabilities, and create a competitive environment for them to make concessions and join the deal, thereby dominating the rulemaking processes. Further, by pursing U.S. digital trade agenda in different rulemaking fora simultaneously or sequentially, U.S.-led forum-shifting proves effective in leveling up the substantive standards, locking in a specific regulatory approach, and getting more countries on board. From KORUS to TPP to USMCA, U.S.-designed digital trade rules have evolved into enhanced protections for transborder data flows, stronger scrutiny on national data restrictive regulations, and greater commitments for an economic approach to data privacy protection. Acclaimed as the "gold standards" for digital trade governance, such data transfer provisions have been increasingly emulated by other countries in their own PTAs,

[752] Wu, *supra* (CJIL), 264.

manifesting prominent “policy diffusion” effect. In this way, the U.S. not only has used PTAs to reshape international trade law based on its digital trade agenda, but also empowers the international trade regime to lay a strong claim to govern the contentious issues of cross-border personal data transfers.

Chapter 3

Forum Shifting to Regulate Data Privacy— The Creation and Evolution of EU Data Protection Regulation

Table of Content

INTRODUCTION 126

I. THE INSTITUTIONAL STATUS QUO ANTE FACING THE EU 133

A. Fragmented National Regulations and the Convention 108 133

B. How Was the Convention 108 (1981) Insufficient? 136

II. VERTICAL FORUM-SHIFTING 1.0: THE CREATION OF THE EU DATA PROTECTION DIRECTIVE 1995 140

A. New Institutionalized Actors Moving the Lawmaking Locus from A Multilateral Treaty to the EU's Unilateral Regulation 140

B. The Role of National DPAs as Norm Entrepreneurs Pushing the Commission to Enact A Supranational Regulation 142

(A) Building Issue-Linkages between Data Privacy Protection and Fundamental European Projects 143

(B) Leveraging Domestic Data Embargo Powers to Alter the Reversion Point 143

(C) Utilizing Expertise and Network Ties to Influence the Shape of the Directive 145

C. The EU Data Protection Directive of 1995 145

(A) Conceptualizing The Right to Personal Data Protection as A Fundamental Right 146

(B) High-Standard Regulatory Controls over Data Processing 147

(C) Strong Controls over Cross-border Transfers of Personal Data 149

(D) Establishing Independent Supervisory Authorities and Institutionalizing Their Transgovernmental Network 153

III. VERTICAL FORUM-SHIFTING 2.0: CONSTITUTIONALIZATION OF DATA PRIVACY PROTECTION AND THE GDPR 154

A. Vertical Forum-Shifting 2.1: Constitutionalization of the Rights to Personal Data Privacy Protection and Privacy 155

(A) Anchoring Personal Data and Privacy Protection into European Constitutional Framework 155

(B) The Normative and Policy Implications of Constitutionalizing Data Privacy Protection 158

B. Vertical Forum-Shifting 2.2: Reforming the EU Directive through the GDPR 160

(A) The Institutional and Political Economic Dynamics underlying the GDPR 161

(a) New Challenges for Protecting Europeans' Personal Data 161

(b) The Prominent Role of the DG Just and WP29 and the Institutional Dynamics within the Commission 162

(c) Geo-political and Geo-economic Considerations 164

(B) The GDPR 165

(a) A Harder Law with an Extended Reach 165

(b) Enhancing Individual Rights to Further Empower Data Subjects 167
(c) Strengthening Corporate Governance by Establishing Collaborative Governance 168
(d) Improving Regulation over Cross-Border Flows of Personal Data 170
(1) The Adequacy Process 171
(2) Alternative Transfer Mechanisms 173
(e) Reinforcing Enforcement Mechanisms 174

IV. TRANSATLANTIC COMMERCIAL DATA TRANSFERS AND ECJ-LED FORUM SHIFTING TO (RE)SHAPE THE "ADEQUACY" STANDARD 175

A. The Safe Harbor Agreement and the ECJ Decision of Schrems I..... 175
(A) The Safe Harbor 176
(B) The ECJ's Decision of *Schrems I* 178

B. The Privacy Shield Agreement and the ECJ Decision of Schrems II..... 183
(A) The Privacy Shield 183
(B) The ECJ's Decision of *Schrems II* 185

C. Implications for International Transfers of Personal Data 189

V. CONCLUSION 191

INTRODUCTION

Hailed as a global leader of data privacy regulation, the EU is famously known for its high-standard data protection rules. In the EU, the rights to privacy and personal data protection constitute inalienable fundamental rights, which are interpreted and enforced by the EU's highest court—the European Court of Justice (ECJ).[753] From the EU Data Protection Directive (the Directive) 1995 to the General Data Protection Regulation (GDPR) 2016, the EU adopts a comprehensive Union-level legislation to regulate data privacy protection and cross-border personal data flows.[754] These supranational laws establish high-standard data privacy principles for both the private and public sectors, enforced and implemented by independent regulatory agencies.[755] In 2016 and 2020, respectively, the ECJ has twice struck down the principal international agreements to transfer personal data from the EU to the U.S., based on violations of fundamental rights of European individuals.[756] Evincing the EU's strong commitments to safeguarding individuals' personal data in the digital era, these notable aspects of the EU data privacy regime raise important questions: why does the EU regulate data privacy (including international personal data transfers) in such distinctive

[753] Charter of Fundamental Rights of the European Union, arts. 7, 8(1), 2000 O.J. C 364/10 ["EU Charter"]; Consolidated Version of the Treaty on the Functioning of the European Union, art. 16 (1), 2010 O.J. C 83/47 ["TFEU"].
[754] European Commission, Directive 95/46/EC, 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, 1995 O.J. (L 281) 31 ["EU Data Protection Directive"]; Regulation 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 ["GDPR"].
[755] See e.g., EU Data Protection Directive, arts. 5-21, 22-26, 28-29; GDPR, arts. 5-50, 51-59, 77-84.
[756] Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct.6, 2015), paras. 73, 96-106 ["*Schrems I*"]; Case 311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020), paras. 198-202 ["*Schrems II*"].

ways, setting it apart from the rest of the world? How did the EU approach evolve in its own trajectory, making European data privacy rules stand out among their peers?[757]

Among a sizable legal scholarship studying the EU's approach to data protection regulation, these questions remain relatively understudied, despite their significant theoretical and practical importance. While conventional legal scholarship offers several explanations for this question, none of them is sufficient.

Many works treat the EU's preference for omnibus, strict data privacy rules as a natural or automatic product of Europe's historical legacies or cultural disposition, exemplified by two influential accounts. First, under a prevalent view, Europeans attached vital importance to protecting their privacy, due to their horrendous experiences with the fascist state intrusion on human dignity during the World War II, as well as pervasive state surveillance in postwar socialist authoritarian countries (like East Germany).[758] These experiences, arguably, have left Europeans more suspicious of mass collection of personal data capable of violating their civil liberties than are citizens in other countries.[759] When faced with privacy concerns created by new computer technologies, the argument goes, Europeans pressed their governments to protect them against systemic abuse of private data, leading to the adoption of strict data privacy rules.[760]

While such authoritarian (or fascist) legacy arguments seem attractive at first glance, this account alone cannot explain the varying national data protection laws among developed democracies in Europe. For instance, while German adopted robust national legislation to protect data privacy in the 1970s, Spain and Italy did not enact data protection laws until the 1990s, notwithstanding these three countries' extensive fascist pasts in the 20th century.[761] Likewise, this line of argument has difficulty accounting for why Sweden and the UK, which did not experience fascist or authoritarian leadership, implemented omnibus, robust data protection rules in the 1970s and 1980s, respectively.[762] Further, this account provides little insights about the substance of EU data privacy rules, the timing of change, or the agents who actively advocated for notable institutional change at the EU level.

---

[757] Under EU law, the right to privacy and the right to data protection are distinct, though partially overlapping, legal concepts. See Meg Leta Jones and Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. R. 93, 97-101 (2021). For the sake of argument, this work uses the term "data privacy" to refer to privacy and data protection.

[758] See e.g., Ramón Mullerat, *EU-US Data Protection: Vindicating Rights to Privacy*, 4 EUROPEAN UNION MIAMI ANALYSIS Papers (June 14, 2017), at 11, http://aei.pitt.edu/8197/1/Mullerat_EUdataLawEUMA2007edi.pdf (tracing the origin of the EU's regulatory approach to data privacy back to Europeans' experiences with fascist governments during the World War II-era and post-War communist regimes); Wolfgang Kilian, *Germany*, in GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION 80-106 (James B. Rule & Graham Greenleaf eds., 2008) (explaining that German's World War II experiences left long-standing intellectual and cultural influences on its data privacy protection policies, making German one of the first countries to adopt comprehensive data protection law); STEWARD A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM (2010). Thomas Shaw, *Privacy Law and History: WWII-Forward*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONAL (March 1, 2012), https://iapp.org/news/a/2013-03-01-privacy-law-and-history-wwii-forward/.

[759] See ANU BRAFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 36 (2020).

[760] See ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 7 (2008).

[761] NEWMAN, *supra*, at 7.

[762] *Id.*

The second account focuses on the legal cultures of Germany and France to explain the origin of European data privacy regime. When comparing the American and European approaches to privacy, James Q. Whitman argued that Europeans conceptualizes privacy as a matter of human dignity (rather than a question of liberty as Americans do), and attributed the drastic differences to two different privacy cultures.[763] Under his account, the European approach to privacy is rooted in ancient French legal notions of honor and human dignity, as well as in Kantian notions of personality under German law.[764] Behind the European conceptualization of privacy resides a core set of value that is strongly oriented towards personal dignity.[765] This value was founded on Europeans' fundamental social and political traditions and developed in Europe's own historical trajectories.[766]

To be sure, Whitman's European dignity arguments are insightful when explaining the origins of German and French privacy laws. Yet, it might be questionable whether these two countries' cultural legacies are transposable to other European nations, and hence, could well account for Europe's preference for privacy protection. As with the authoritarian legacy arguments, Whitman's theory cannot adequately explain the cases of the UK (an Anglo-Saxon European country with a drastically different legal culture) that enacted German-like data protection law, and other continental Europe countries lacking national data protection laws before the 1990s (including Italy, Spain, Belgium, Portugal, Greece).[767]

Further, if subsequent institutional trajectories are completely preordained by ancient legal legacies, it is hard to explain the U.S. case either. While the legal concept of the "right to privacy" was developed by U.S. jurists in 1890[768] and has been widely regarded as one of the most seminal notions in U.S. privacy law,[769] the U.S. did not follow the EU approach to adopt a comprehensive data privacy regime. The 1974 U.S. Privacy Act, being the only federal omnibus act protecting information privacy, only applies to data processing activities of the federal government, rather than state governments or the private sector.[770] On the private sector, the U.S. has long maintained a sectoral, piecemeal approach to regulate targeted, sensitive sectors only (including banking, health care, children's online privacy, video rental business), and primarily relies on industry self-regulation and market mechanisms to protect individuals' data privacy.[771] In short, to the extent that historical or cultural factors are treated as casual mechanisms or independent variables leading to concrete policy outcomes, their force of explanation often seems indeterminant and ambiguous.[772] While the authoritarian legacies or ancient dignity arguments can help to contextualize our

[763] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L. J. 1160 (2004).
[764] *Id*., at 1172-89.
[765] *Id*. 1220.
[766] *Id*. 1219.
[767] See *id*., at 35.
[768] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. R. 193 (1890).
[769] Benjamin E. Bratman, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENNESSEE L. R. 623, 623-6 (2002). Brandeis and Warren's contribution as such "has been widely recognized by scholars and judges, past and present, as *the* seminal force in the development of a "right to privacy" in American law." See *id.*, at 624.
[770] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22-3 (2000) ["*Globalization and Social Protection*"].
[771] Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STANFORD L. REV. 1315, 1331 (1999) ["*Resolving Conflicting*"].
[772] See SVEN H. STEINMO, AMERICAN EXCEPTIONALISM RECONSIDERED: CULTURE OR INSTITUTIONS? 107 (1994).

understanding about the EU's policy choice, they alone come up short in explaining the EU's salient preference for strict supranational data privacy regulation.

A more sophisticated account emphasizes the role of powerful EU member states (that were early adopters of strict national data protection laws) in externalizing their domestic regulatory frameworks through EU legislation. Following the classical "two-level" game model of liberal intergovernmental theory, this argument focused on the national economic interests of the most powerful EU member states to explain regional institutional change.[773] Under this view, the domestic firms from these countries suffered from a competitive disadvantage when competing in the European market, because many other EU member states at the time had laxer or no national data protection laws (including large markets, such as Italy and Spain).[774] To level the playing field for their own domestic companies, the French and German governments successfully pushed for a supranational regulation at the EU level, requiring all member states to enact equivalent domestic data privacy laws.[775] To that end, these powerful member states had leveraged their huge economic clouts (derived from their large domestic markets) and political powers to project their policy preferences at the EU level, influencing the EU's decision-making on their preferred terms.[776] And the argument continues that the bureaucratic interests of the European Commission (Commission) also facilitated this process of regional rulemaking, paving the way for regulatory change. To the Commission, supporting pan-European data protection regulation aligned with its own institutional interests, since such a legislation can expand its competence in the emerging information society and broaden its mandate of supranational decision-making.[777]

While offering a seemingly potent explanation for the origin of EU data protection law, this theory can barely withstand the scrutiny of key historical facts. Contrary to what this account suggests, in fact, for much of the 1980s, both the national governments and business interest groups of Germany, France, and the UK—the largest EU member states with stringent data protection laws—showed little interest in lobbying for an EU legislation to regulate data privacy, instead generally concurring that national regulations should be the primary institutional solution.[778] For instance, the German industry showed a notable disinterest in pursuing a supranational regulation to harmonize domestic data protection laws across EU member states, despite their potential economic gains from an upward regulatory harmonization, largely due to the concerns that such a law may exacerbate the

---

[773] Abraham L. Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, 62 INT'L ORGAN. 103, 106, (2008) (explaining a liberal intergovernmental argument: "preferences of national economic actors drive the negotiating position of each member state. These economic preferences are aggregated nationally and represented at the European level by a unitary national executive. The relative economic and broader political power of the nation, then, determines the ability of a government to achieve its domestic national preferences at the supranational level").

[774] NEWMAN, *supra*, at 7. See generally DAVID VOGEL, TRADING UP: CONSUMERS AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1995).

[775] See Ulrich U. Wuermeling, *Harmonisation of European Union Privacy Law*, 14 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW 411 (1996); Nick Platten, *Background to and History of the Directive*, in EC DATA PROTECTION DIRECTIVE (DAVID BAINBRIDGE ED., 1996).

[776] Newman, *supra*, at 106. See generally ANDREW MORAVCSIK, THE CHOICE FOR EUROPE: SOCIAL PURPOSE AND STATE POWER FROM MESSINA TO MAASTRICHT (1998) (emphasizing the importance of powerful EU member states' national preferences in influencing European policymaking).

[777] Newman, *supra*, at 107.

[778] *Id*., at 111-2.

fragmentation of the EU market.[779] Concerned with potential adverse impacts (including adjustment costs) on businesses, major transnational business interest groups in Europe also strongly opposed a supranational data protection legislation.[780]

This indifferent or even resistant attitude was shared by large member state governments and the Commission. Neither the German nor the French governments had actively lobbied for a pan-European data privacy law that might alter their own national rules.[781] And the British government was the most vocal opponent of such a European regulation, arguing that it may undermine economic growth and burden public administration.[782] By the mid-1980s, the Commission, too, had repeatedly rejected an EU directive to harmonize national data privacy regulations, despite its huge agenda-setting powers to pursue EU legislation.[783] Rather, the Commission supported the industry's proposals to rely on national regulations to deal with this area.[784] Given the manifest lack of interest by the business groups, large member states, and the Commission to press for supranational data privacy lawmaking, why the EU passed the Data Protection Directive in the early 1990s after years of inaction seems pretty much an empirical puzzle.[785]

In addition, this account encounters other problems as well. Given that the EU's data privacy regime continues to evolve since the enactment of the Directive, this theory cannot explain why the EU sought to upgrade the rights to personal data protection and privacy to part of EU primary law by the late 2000s, anchoring them into European constitutional framework.[786] Neither can it account for why the Commission suddenly accelerated its efforts to push through the GDPR to replace the Directive since 2009, despite more than a decade of reluctance and inaction to reform EU data protection framework.[787] Finally, heavily focused on the economic interests of powerful member states, this account neglects the important role of the ECJ in shaping the EU's data privacy rules and international data transfer mechanisms, which tends to prioritize human rights over competing commercial interests underlying personal data.[788]

In light of the deficiencies of existing theories and arguments, this chapter advances a different analytical framework to explain the creation and evolution of EU data privacy regime. Drawing on

[779] *Id*., at 112 (noting that a representative of the Germany's largest trade association in 1989 stated that the Germany industry did not endorse a European data privacy legislation, despite the resultant economic costs to them; and that a survey conducted by the German private-sector data protection trade association showed that 91% of the 255 participating firms (from a wide range of different sectors and of distinct firm sizes) thought that EU data privacy regulation will worsen market fragmentation across different member states).
[780] *Id*., at 111.
[781] *Id*. (noting that the German interior minister argued for national laws to regulate data privacy, due to the sensitive nature of domestic business and public security demands).
[782] *Id*.
[783] *Id*., at 110-1 (noting that the Internal Market Directorate of the Commission considered data privacy as primarily a public-sector issue involving member states' government data-banks, and to the extent that data protection concerns the private sector, it resisted European data privacy rules, out of the fears that such a harmonization would increase regulatory costs and undermine business interests).
[784] *Id*., at 111.
[785] *Id*., at 104-5.
[786] See *infra* Section III.A(A).
[787] See *infra* Section III.B(A).
[788] See *infra* Section IV.

international relation (IR) scholarship on forum shifting,[789] it conceptualizes the existence of this legal regime as a result of contentious supranational lawmaking processes, whereby a set of privacy-oriented institutional actors with a shared policy preference leveraged different decision-making fora to advance their policy preferences and alter existing institutional rules. Approaching EU data protection law as legal processes beyond back-letter-law, this chapter hopes to reveal prominent power dynamics underlying the EU's supranational lawmaking activities and shaping the legal and policy outcomes. In so doing, I distinguish this work from existing scholarship on two major aspects.

First, through the theoretical lens of regime- and forum-shifting, this chapter hopes to capture the evolving, iterative lawmaking processes leading to EU data privacy regime as it currently stands, focused on important power dynamics to explain the adoption, timing, and content of the rules being made. As a policy change strategy, "regime shifting" (or "forum shifting") enables an actor to strategically move international treaty negotiations, lawmaking processes, or standard-setting initiatives from a *status quo* venue to an alternative one that is more aligned with its preferred interests, in efforts to reshape institutional rules governing an issue-area.[790] International lawyers and legal scholars often undertheorize such competitive lawmaking strategies adopted by states, institutions, or non-state actors to influence transnational rulemaking or international regulation of an issue-area based on their preferences. Due to this largely missed perspective, however, many dynamics are lost in the case of EU data privacy regime.

Far from being predetermined by authoritarian experiences or ancient dignity legacies, EU data protection lawmaking is characterized by legal contestations that occurred back and forth among multiple, partially overlapping venues, providing opportunity structures for a set of institutional actors to mobilize, contest, advocate, cooperate, and coordinate, in pursuit of their joint agenda.[791] Sharing a common preference for strong data privacy protection, these actors include, most notably, national data privacy authorities (DPAs), their transgovernment network (the Article 29 Working Party ("WP29")), the Directorate-General for Justice and Consumers ("DG Just", a rights-oriented department of the Commission), the ECJ, and the European Court of Human Rights (ECtHR). By leveraging their various power resources at hand, these protagonists sought to create, (re)interpret, reinforce, expand, and reform EU data privacy rules, continuously driving institutional change and development at the EU level for decades. In addition to revealing the dynamic lawmaking processes at work, this lens is particularly relevant to explain why the EU has been regulating data privacy in such ways as to empower the mandate, competence, and authority of national DPAs, their

---

[789] JOHN BRAITHWAITE & PETER DRAHOS, GLOBAL BUSINESS REGULATION 564-5 (2000); Julia C. Morse & Robert O. Keohane, *Contested Multilateralism*, 9 REV. INT'L ORGAN. 385, 388, 392-3 (2014). Laurence R. Helfer, *Regime Shifting in the International Intellectual Property System*, 7 PERSPECTIVES ON POLITICS, 39 (2009); Laurence L. Helfer, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking,* 29 YALE. J. INT'L L. 1 (2004) ["YJIL"]; Susan K. Sell, *TRIPS Was Never Enough: Vertical Forum Shifting, FTAs, ACTA, and TPP*, 18 J. INTELL. PROP. L. 447 (2011).

[790] Broadly speaking, "regime shifting" contains two scenarios. The first is "*inter-regime shifting*" or "*horizontal regime shifting*", which relocates the decision-making processes from one international regime to a different regime. The second is "*intra-regime shifting*" (also known as "*forum shifting*"), concerning a shift of the policy-making processes to another venue located within the same regime. "*Intra-regime shifting*" includes "*vertical forum shifting*", referring to strategic efforts to shift the lawmaking initiatives from a multilateral venue to unilateral, bilateral, or plurilateral fora below the multilateral level. See Helfer, *supra* (YJIL), at 14, 16; Sell, *supra*, at 451.

[791] See HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 29 (2019). See *infra* Parts I to IV.

transgovernmental network, and the ECJ in their oversight, enforcement, and application of EU data protection law.

Second, unlike many "state-centric" international law or IR literature, this chapter focuses on an important, yet understudied, role of sub-national and supranational institutions in serving as "norm entrepreneur" and driving transnational lawmaking. Overall, existing scholarship on regime- and forum-shifting tends to focus on lawmaking initiatives launched by sovereign actors.[792] Under the prevalent realism theory, powerful states (particularly great powers) typically dominate the international governance processes, since they can leverage their asymmetrical powers (including market powers, political influence, and material capacities) to externalize their preferred policies on other countries, irrespective of the latter's own preferences.[793] Even when they could not prevail at a specific international institution or forum, major powers are adept at shifting the decision-making procedures to an alternative venue more amenable to their interests, shaping the rule-making outcomes based on their preferred terms.[794]

Contrary to this traditional account, this chapter shows that institution-led forum-shifting, too, can be dominant in pursuing normative and strategic goals, at least in the case of EU data privacy regime. Rather than a result imposed by powerful EU member states for their national economic interests, the creation and development of EU data protection law reflect the contentious lawmaking processes, led by sub-national and supranational institutional actors that remain relatively independent from member states and retain their distinct policy preferences. While states remain predominant in the international arena, sometimes a powerful state or even a superpower does not have a straightforward preference on an issue-area (or is torn among different preferences), opening the window for institutions to advocate for their cause and project their preferences on key decision-makers at the supranational level. These insights help to remedy the relative omission in existing regime-shifting literature, offering a counterweight to scholars' preoccupation with nation-states.

By moving the emphasis from states to institutions (below or above the nation-state level), this study is conducive to unveiling the intricate power dynamics pervading transnational privacy lawmaking. Specifically, it helps to dispel the often-taken-for-granted illusion that the EU is a unitary sovereign actor particularly obsessed with privacy, human rights, and rule of law. In fact, neither the EU nor its member state is "unitary" when it comes to data privacy lawmaking. Rather than a homogenous entity with a fixed preference for strict privacy rules, the EU is composed of different institutions (both at the EU and member state levels) with different normative and policy goals and decision-making processes.[795] For instance, while the Directorate General for international trade ("DG Trade",

[792] See Helfer, *supra* (2009); Helfer, *supra* (2004); Sell, *supra*; Eyal Benvenisti & George Downs, *Political Economy and the Fragmentation of International Law*, 60 STANFORD L. R. 595, 595-6 (2007).
[793] See e.g., Daniel W. Drezner, *The Power and Peril of International Regime Complexity*, 7 PERSPECTIVES ON POLITICS 65, 66-7 (2009).
[794] DANIEL W. DREZNER, ALL POLITICS IS GLOBAL: EXPLAINING INTERNATIONAL REGULATORY REGIMES 63-4, 67 (2007) ("While all states will attempt to select for amenable to their interests, great powers will have the greatest success of employing this tactic").
[795] Sveltlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV., 416, 478 (2020).

the trade department of the Commission)[796] may favor reaching a commercial agreement to transfer personal data with an important foreign trade partner to facilitate trade flows, the Directorate General for Justice and Consumers ("DG Just", the Commission department for EU policy on justice and consumer rights)[797] could prioritize EU law reform to reinforce personal data protection, national DPAs can actively launch regulatory investigations over multinational digital giants' data processing practices and challenge them before national courts, and the ECJ might choose to intervene sometimes to scrutinize the legality of international data transfer mechanisms (adopted by the Commission) under EU constitutional law. Through this lens, the EU's lawmaking processes on data privacy feature long-standing political and legal battles between pro-civil-liberties actors and their opponents favoring other interests underlying personal data, with their power balance shifting over time. As such, this chapter aims to provide a textured account of the power dynamics at the transnational level, enriching our understanding about the politics behind the emergence and evolution of EU data privacy regime.

The remainder of this chapter proceeds as follows. Part I gives a brief overview of the national and regional regulatory frameworks preceding the creation of EU data protection regulation, demonstrating how pre-existing institutional rules were unable to adequately resolve the regulatory issues faced by the EU. Part II traces the lawmaking process leading to the EU Data Protection Directive, whereby national DPAs leveraged their power resources to shift the rulemaking locus from a multilateral convention to the EU's unilateral legislative acts. Part III proceeds to explore how a set of pro-civil-liberties institutions sought to anchor data privacy protection into European constitutional order and to reform the Directive by enacting the GDPR. Part IV discusses how EU data protection law has substantially shaped transatlantic commercial data transfers, focused on the ECJ's forum-shifting initiatives to redefine the "adequacy" standard. Part V summarizes and draws conclusive remarks.

I. THE INSTITUTIONAL STATUS QUO ANTE FACING THE EU

Before delving into the major lawmaking processes generating EU data protection law, this Part briefly reviews the institutional frameworks prior to such initiatives. Section A summarizes the European national data protection laws in the 1970s and 1980s, and introduces the efforts of European data privacy experts to advocate for an international treaty from the Council of Europe. Section B discusses how the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as one of the most influential first-generation international data privacy instruments, failed to provide a satisfactory regulatory solution to the problems faced by EU member states.

A. Fragmented National Regulations and the Convention 108

As technological developments enabled computer-driven monitoring systems and automatic data processing, advanced industrial democracies confronted novel regulatory issues on individuals'

[796] European Commission, *Directorate General for Trade*, https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/trade_en ("This Commission department is responsible for EU policy on trade with countries beyond the EU's borders").
[797] European Commission, *Directorate General for Justice and Consumers*, https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/justice-and-consumers_en.

data privacy protection.[798] Faced with common threats of massive surveillance by governmental bodies and private firms, national governments in Europe, however, came up with divergent regulatory frameworks. By the late 1970s, European national data privacy regimes can be broadly grouped into three categories.[799]

First, France, Germany, Luxembourg, Sweden, Denmark, Norway, and Austria adopted a comprehensive data privacy regime with relatively stringent data privacy rules for the public and private sectors.[800] Under such laws, independent regulatory agencies (i.e., national DPAs) were established to enforce data privacy rules and monitor their implementation.[801] And many of these agencies were endowed with "data embargo" powers—the authority to block transfers of personal data to countries or firms that failed to maintain adequate data privacy protection.[802] Second, there were countries, like Switzerland, that adopted a sectoral data privacy regime. Such a limited regime adopted some sectoral laws to regulate personal data in sensitive industries (such as financial and health data), but primarily relied on business self-regulation to protect data privacy in the private sector.[803] Third, Italy, Belgium, Greece, Spain, Portugal did not adopt national data privacy laws at all.[804] As noted by Abraham Newman, "member states of the European Community thus entered the 1980s with very different regulatory systems."[805] And in the second half of the 1970s, a growing number of European countries enacted national data privacy laws that authorized local regulatory authorities to restrict or block cross-border personal data flows to countries without similar levels of data privacy protection, addressing the risks of offshore "data havens".[806]

In this context, an epistemic community, mainly consisting of national data privacy experts, emerged in the 1970s and entered the political arena, in pursuit of an agenda to advance data privacy protection.[807] With shared belief in the importance of data privacy protection, this community was concerned with the threats imposed by computer technology on European citizens' civil liberties, and the dangers associated with international personal data transfers.[808] The absence of data privacy laws in many EU member states not only failed to provide sufficient protection for Europeans' data privacy in the context of automatic data processing, but also may create offshore "data havens", facilitating circumvention of stringent national privacy regulations in other European countries.[809] In response, these data privacy experts lobbied European institutions,

[798] Newman, *supra*, at 108.
[799] *Id.*
[800] *Id.* A. C. Evans, *European Data Protection Law*, 29 AM. J. COMP. L. 571, 571-72 (1981).
[801] Newman, *supra*, at 108-109 (noting that under the institutional design, national data protection authorities were shielded from direct government influence, composed of civil servants and political leadership with extended tenure, and guaranteed a minimum budget).
[802] *Id*., at 109. See DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989).
[803] Newman, *supra*, at 109.
[804] *Id.*, at 110.
[805] *Id.*, at 109.
[806] LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 34 (2014).
[807] Newman, *supra*, at 108 (noting that "[a]s European countries considered national legislation in the early 1970s, data privacy experts from European countries met internationally to discuss the implications of cross-border data flows for personal privacy… feared that unconstrained technology would threaten the civil liberties of European citizens").
[808] Newman, *supra*, at 109.
[809] *Id.* BYGRAVE, *supra* (DATA PRIVACY LAW), at 34.

calling for pan-European rules to regulate data privacy protection and transnational personal data flows.[810]

The results were mixed. The European Commission had little interest in data privacy regulation in the 1970s, for fear that doing so may raise the costs of doing business in Europe and that such regulation was a public-sector issue beyond its jurisdiction.[811] Instead, the Commission considered that protection of data privacy with respect to computer data banks was "basically" a matter for member states to address, and that its primary normative concerns were to ensure that its own institutions would not breach data privacy.[812] Such an attitude indicates that the Commission's initial policy priorities were to develop the internal market and a European computer industry, as opposed to safeguarding individuals' human rights of data privacy.[813]

In contrast, the European Parliament was more amenable to data privacy experts' concerns. Concerned with protecting human rights against new technological developments, the Parliament was initially the most active institutional actor on this issue.[814] In addition to the importance of data privacy protection per se, there was more dynamics behind this stance. In the early 1970s, the Parliament, eager to respond to the allegation that the Community undermined the rights enjoyed by European citizens under national constitutions, hoped to show that EU law can safeguard human rights against the acts of national governments and private firms in member states.[815] In this context, data privacy protection presented an ideal issue-area for the Parliament to protect the civil liberties of European citizens.[816] In 1973 and 1974, through its Legal Affairs Committee, the Parliament released two reports on data privacy protection, emphasizing the need for the European Community to serve as a guardian of human rights and to protect individuals' data privacy.[817] Also, the Parliament passed several resolutions, repeatedly calling for a pan-European data protection regulation.[818]

The most congenial forum to advance data privacy experts' causes proved to be the Council of Europe (CoE). An international organization devoted to advancing human rights, the rule of law, and democracy,[819] the CoE demonstrated strong concerns for individuals' data privacy protection

---

[810] Newman, *supra*, at 109.
[811] *Id.*
[812] Evans, *supra*, at 574.
[813] *Id*., at 574-75 (explaining that at the time, the Commission aimed to promote a European computer industry (which may be impeded if different member states enacted their distinct rules for data privacy protection), and was concerned that divergent national data privacy rules may create problems for firms whose business model hinged on cross-border transfer of personal data, and would seriously distort internal trade within the Community).
[814] BYGRAVE, *supra* (DATA PRIVACY LAW), at 54.
[815] Evans, *supra*, at 575 (noting that such an accusation "culminated in the ruling of the West German Constitutional Court of 29 May 1974". Id. fn. 20 (1974 2 *C.M.L.R.* 540, at 552).
[816] FRITS W. HONDIUS, EMERGING DATA PROTECTION IN EUROPE 72-73 (1995) (arguing that "this subject was ideally suited to demonstrate that the European Communities, and especially the Parliament, were doing something to defend the fundamental freedoms of the individual Community citizen"); Evans, *supra*, at 575 (noting that "[t]his motive seems to have influenced the Parliament's approach to data protection").
[817] Couste Report, E.P. Doc. 153/74, at 23; Mansfield Report, E.P. Doc. 487/74, at 9; See Evans, *supra*, at 575.
[818] European Parliament Resolution [1975] O.J. C60/48, [1976] O.J. C100/27, [1979] O. J. C140/34; [1982] O. J. C 87/39. See BYGRAVE, *supra* (DATA PRIVACY LAW), at 54.
[819] The Council of Europe (CoE) is not to be confused with the Council of the European Union (the Council), or the European Council. Distinct from the European Union (EU), the CoE is an international organization founded by European countries in 1949 to uphold and promote human rights, democracy, and the rule of law in Europe. The

and civil liberties.[820] After a debate on implications of modern technologies for individuals' privacy in 1968, the Consultative Assembly of the CoE held that member states' national legislations and the European Convention on Human Rights (ECHR) provided inadequate legal protection for individuals data privacy.[821] In the early 1970s, the CoE set forth a specialist committee, mainly composed of national data privacy experts, to study how to regulate data protection in light of technological advancements.[822] Drawing on the models of several national (and sub-national) data privacy laws, the specialist committee made two major recommendations concerning the proper use of personal data in both the private and public sectors, which were approved by the Committee of Ministers of the CoE in 1973 and 1974, respectively.[823] In 1974, the CoE showed a political will to establish minimum standards governing the public and private sectors' data processing.[824] Subsequently, these two recommendations were incorporated into the basic data privacy principles of the Convention 108, which was adopted by the CoE in 1981.[825]

B. Assessing the Convention 108 (1981)

The Convention 108 represents the highlight of the normative response in the 1980s to stimulate national laws to protect data privacy, harmonize domestic regulations, and maintain free flows of personal data across national borders.[826] An important milestone in the development of data privacy protection as a fundamental right,[827] the Convention codified a set of fair information practices to safeguard data privacy, providing a high-level framework of basic principles governing the processing of personal data.[828] While not ground-breaking in themselves, these

---

Council, composed of the government ministers of each EU member state, is the major legislature body of the European Union. See Council of Europe, *Values: Human Rights, Democracy, Rule of Law*, https://www.coe.int/en/web/about-us/values; Council of the European Union, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/council-european-union_en. Composed of the heads of EU member states, the European Council is an EU institution that "defines the general political direction and priorities of the European Union", but it lacks the authority to legislate, https://www.consilium.europa.eu/en/european-council/.

[820] Evans, supra, at 575 (noting that for example, in March 1974, "[i]n Reply to an Oral Question by Mr. Couste, another M.E.P., Council President-in-Office Appel expressed the view that 'the primary aim was to protect private life'… and The Council was, then, apparently ready to approve action by the Community itself in the field of data protection, provided this were shown to be the more practical means of protecting individual privacy").

[821] *Id*., 572-73 (noting that while article 8 of the ECHR provides the right to privacy, this treaty was crafted in 1950, and hence, far before threats imposed by computer-driven monitoring systems and data banks to human rights emerged; and that article 8 only covers the public sector, but "a considerable proportion of existing data banks are operated by private firms").

[822] Newman, *supra*, at 110.

[823] Evans, *supra*, 573 (noting that the specialist committee produced draft Recommendations on the Protection of Individuals vis-à-vis Electronic Data Banks in the Private Sector (Recommendation (73) 22) and on the Protection of Individuals vis-à-vis Electronic Data Banks in the Public Sector (Recommendation (74) 29)). BYGRAVE, *supra* (DATA PRIVACY LAW), at 33 (noting that such models included the data privacy laws of Germany (i.e., the state of Hessen) and Sweden).

[824] Evans, *supra*, at 573-74.

[825] Newman, *supra*, at 110.

[826] BYGRAVE, *supra*, at 34.

[827] Convention 108, preamble; art. 1 ("The purpose of this convention is to secure in the territory of each Party for every individual… respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data…"); CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 37 (2013).

[828] COLIN J. BENNETT, REGULATING PRIVACY 133-36 (1992).

principles "established a key reference point for subsequent elaborations of data privacy principles in both international and national instruments."[829] In addition, the Convention included provisions to regulate data transfers between its contracting states,[830] aimed to facilitate cross-border data flows essential for international trade.[831] As the only multilateral treaty specifically dealing with data privacy protection, the Convention had nineteen countries acceded to it by the mid-1990s.[832] However, it also had important gaps and limitations, undermining its effectiveness in practice.

First, the substantive data privacy principles of the Convention often feature general formulations with a flexible nature, undercutting its effects in harmonizing national data protection regulations. Typically, the basic principles of data privacy protection are formulated in a relatively general and abstract manner, with many core concepts undefined by the Convention and its Explanatory Report.[833] Also, the Convention allows discretionary derogations, exceptions, and restrictions on the implementation of such principles.[834] While facilitating acceptance by different member states with different political, legal, economic, social, and cultural character, these features constrain the capacity of the Convention to prevent divergence in national data privacy laws and to provide operational "rules for the road" in concrete scenarios.[835]

For instance, article 3(2)(a) allows a contracting state not to apply the Convention to certain categories of automatic data files, if the latter are not protected under its own domestic law.[836] While this provision helps to ensure that variations in national regulations do not constitute trade barriers in Europe, its invocation by a contracting state can result in a serious restriction in individuals' data privacy protection, and is of little avail in harmonizing national data privacy laws.[837] While the Convention establishes a valuable set of basic principles for data privacy protection, the undefined, vague terms used in core provisions[838] and the broad exceptions, derogations, and restrictions allowed with respect to data privacy protection[839] may significantly undermine effective implementation of this treaty.[840]

Second, the Convention does not have strong enforcement mechanisms. A "non-self-executing" treaty, Convention 108 requires contracting states to enact national data privacy laws to give effect

[829] BYGRAVE, *supra*, at 36.
[830] Convention 108, art. 12.
[831] Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHICAGO L. R. (forthcoming 2023), at 12, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531.
[832] *Id.*
[833] BYGRAVE, *supra*, at 40. For example, the undefined terms of "*appropriate safeguards*" in articles 6 and 7 and "*appropriate sanctions and remedies*" in article 10 of the Convention are vague and ambiguous, leaving a considerable margin of discretion to member states to implement these provisions. See Evans, *supra*, at 578-79; see also Convention 108, arts. 6-7, 10.
[834] BYGRAVE, *supra*, at 41. See Evans, *supra*, at 579-80 (noting that under article 9, the key grounds that permitted member states to derogate from basic data privacy principles are undefined and vague, including "protecting State security, public safety, the monetary interests of the State or the suppression of criminals offences" as well as "protecting the data subject or the rights and freedoms of others"); cautioning that "absence of any definition of these grounds could lead to abuse"); see also Convention 108, arts. 3, 6, 9.
[835] BYGRAVE, *supra*, at 41.
[836] Convention 108, arts. 3(2)(a).
[837] Evans, *supra*, at 578.
[838] E.g., Convention 108, arts. 6-7, 10.
[839] E.g., Convention 108, arts. 3(2), 9.
[840] Evans, *supra*, at 580.

to its principles.[841] Yet, the Convention does not establish specialized institutions to oversee and enforce its implementation.[842] Indeed, it contains provisions requiring the establishment of authorities to help oversee its implementation and maintain a high level of mutual assistance.[843] But without specifying minimum requirements on their competence, independence, and functions, these provisions fall short of mandating the establishment of independent regulatory agencies in the form of national DPAs.[844] Neither can this gap be filled by the Consultative Committee, which only has an advisory mandate.[845]

In addition, since membership of Convention 108 does not give rise to the jurisdiction of the European Courts of Human Rights (ECtHR), there is no direct judicial enforcement of the Convention.[846] In this regard, it is worth noting two caveats. First, the ECtHR has referred to Convention 108 in some cases, and article 8 (the right to respect for a private life) of the ECHR may give rise to the obligation to give effect to the provisions of Convention 108.[847] Second, breaches of Convention 108's basic data privacy principles may constitute an interference with article 8 of the ECHR, and thus can fall into the jurisdiction of the ECtHR.[848] However, due to the heavy caseload and procedural limitations (e.g., the exhaustion of local remedies), the ECtHR are unable to ensure effective oversight and robust enforcement of the Convention.[849] Plus, not all breaches of the basic principles of Convention 108 may qualify as a breach of the ECHR.[850]

Third, when regulating cross-border flows of personal data, the Convention does not provide a uniform set of standards for national governments to restrict or prohibit data transfers. Under article 12, the Convention generally allows international transfers of personal data between its contracting states, meanwhile giving national governments discretionary powers to restrict or ban data flows in limited circumstances.[851] Given European countries' divergent approaches to data privacy and cross-border data transfers at the time, the Convention, however, does not create a supranational consensus on the conditions to limit or block data flows, but largely defers to the decision-making of national authorities. For example, a contracting state with strict data privacy law may invoke such derogations to block transfers of personal data to other contracting states

---

[841] BENNETT, *supra*, at 135.
[842] BYGRAVE, *supra*, at 39-40.
[843] Convention 108, ch. IV, arts. 13-17.
[844] BYGRAVE, *supra*, at 39.
[845] *Id.*, at 40. See Convention 108, ch. V, arts. 18-19.
[846] KUNER, *supra*, at 37.
[847] *Id.* Drafted by the CoE, the ECHR is an international treaty to protect human rights in Europe. All CoE member states are parties to this treaty, and the ECtHR oversees its implementation. See A Convention to Protect Your Rights and Liberties, https://www.coe.int/en/web/human-rights-convention.
[848] BYGRAVE, *supra* (DATA PRIVACY LAW), at 40 (noting that the Convention 108 "is clearly envisaged as an elaboration of the protection provided under ECHR Article 8, and ECtHR confirms this").
[849] *Id*.
[850] *Id*.
[851] The Convention generally prohibits contracting states from banning transnational personal data transfer or subjecting that to special authorization for the sole purpose of privacy protection, establishing the default rules of cross-border data flows among contracting states. This is subject to two narrowly tailored exceptions. First, a contracting state may derogate from that rule, where its legislation contains specific regulations for certain categories of personal data or automated personal data files, and the recipient country has no equivalent protection. Second, derogation is also allowed, if transfers of personal data is made from the intermediary of a contracting state to a non-contracting state, in order to circumvent the legislation of the former. See Convention 108, art. 12(2)-(3).

whose data privacy laws they deemed inadequate.[852] In that case, the objective of maintaining free personal data flows between contracting states would still be impeded.

Fourth, the Convention contains no rules to regulate cross-border flows of personal data to a non-contracting state. Though seemingly trivial from the outset, this gap makes this treaty increasingly out of touch with modern-day business practices featuring frequent and constant transfers of data across different jurisdictions.[853] While the Convention textually allows ratification by states that are not members of the CoE,[854] this possibility remains unexplored for more than two decades after its enactment.[855] Also, accession by such non-member states to the Convention is politically demanding, as it requires the unanimous vote of contracting states' representatives sitting on the Committee of Ministers.[856] Given that most of non-contracting states had not adopted a European-like data privacy law at the time (and hence can potentially serve as "data havens"), it is doubtful how the Convention (as it stood in the 1980s) can achieve its asserted policy goal: to prevent data controllers from circumventing applicable data privacy standards by moving data-processing operations to jurisdictions with lax or no protections.[857]

Fifth, the Convention received only a lukewarm response from CoE member states at the time. By the end of the 1980s, only nine member states had ratified the Convention.[858] While it prompted data privacy debates among legislators in the UK, a third of the European Community did not adopt national data privacy laws in response to the Convention.[859] Spain even failed to do so, after it ratified the Convention in the early 1980s.[860] This situation reflects the failure of the Convention to lead contracting states to adopt comprehensive and high-standard data privacy laws.

As a result, the Convention did not effectively address the policy challenges imposed by cross-border data flows in Europe. Notably, the European policy network of data privacy experts that pushed the CoE to set the Convention's agenda lacked the powers to ensure its implementation by national governments.[861] And even assuming all European countries were willing to ratify the Convention, it is still far from clear how it can provide individuals with sufficient protection of their data privacy, harmonize national regulations, ensure cross-border personal data flows, or prevent the emergence of "data havens" within Europe.[862] With the failure of the Convention to

[852] Evans, *supra*, at 580-81.
[853] Chander and Schwartz, *supra*, at 38.
[854] Convention 108, art. 23(1).
[855] Lee A. Bygrave, *The "Strasbourg Effect" on Data Protection in light of the "Brussels Effect": Logic, Mechanics and Prospects*, 40 COMPUTER LAW & SECURITY REVIEW 1, 1 (2021) (noting that "[i]t was not until 2008 that the Council began to push the Convention as potentially more than an agreement between European countries, and even then the Council's initial moves were 'tentative'").
[856] Convention 108, art. 23(1).
[857] Explanatory Report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (January 28, 1981), para. 9 [Explanatory Report on Convention 108]. But in 2001, an Additional Protocol to the Convention introduced more details rules to regulate international personal data transfers to a non-member state. See KUNER, *supra*, at 38.
[858] Newman, *supra*, at 110 (noting that the countries that ratified the Convention prior to 1990 "included Austria, Denmark, France, Germany, Luxembourg, Norway, Spain, Sweden, the United Kingdom").
[859] *Id.*
[860] *Id.*
[861] *Id.*
[862] Evans, *supra*, at 580. BYGRAVE, *supra* (DATA PRIVACY LAW), at 55 (noting that in 1990, the Convention "failed to establish more than a minimal, formal equivalence between the national data privacy laws of the Federal Republic

ensure widespread enactment of national data protection laws across Europe by the mid-1980s,[863] data privacy advocates turned to other European institutions (most notably, the European Commission), in order to forge new political campaigns to alter the *institutional status quo ante*.

II. VERTICAL FORUM-SHIFTING 1.0: THE CREATION OF THE EU DATA PROTECTION DIRECTIVE 1995

This Part explores how national DPAs utilized the strategy of vertical forum-shifting to push for the enactment of the EU Data Protection Directive. Section A analyzes the strategic considerations underlying the choice of the lawmaking forum by the transformed data privacy network. Section B charts how these actors leveraged their power resources to impose their policy preferences on the European Commission. Section C briefly reviews the Directive, showing how this legislation regulates personal data protection and cross-border data flows.

A. New Institutionalized Actors Moving the Lawmaking Locus from A Multilateral Treaty to the EU's Unilateral Regulation

During the 1980s, as a growing number of European countries had established national data protection authorities, the data privacy community was transformed from an epistemic community (primarily composed of legal experts) to an institutionalized group of independent regulatory agencies, which became politically powerful data privacy advocates.[864] As the oversight and enforcement mechanisms, DPAs were vested with regulatory authority and law enforcement powers to monitor and implement domestic data privacy rules.[865] With the delegated competence to protect data privacy and substantial statutory buffers to direct political control, these regulatory agencies developed policy preferences distinct from their national governments.[866] Through routine transgovernmental cooperation (such as annual conference of European data privacy commissioners) over a ten-year period, these actors built network ties with each other across different member states, and came to formulate a coherent proposal for pan-European data privacy regulation.[867] Motivated by a shared belief in the importance of data privacy protection and their concerns that European "data heaven" countries would undermine national protection levels and endanger their regulatory authority, national DPAs sought to establish a European-wide comprehensive data privacy regime with high-standard protection.[868]

---

of Germany, France, the UK, and the Netherlands. This meant that the free flow of personal data between a large number of EU states could not be guaranteed").

[863] Newman, *supra*, at 109-110.

[864] *Id.*, at 112 (noting that "[a]s negotiations began in 1976 over the Council of Europe Convention, only one country, Sweden, had a national data privacy authority. By the end of 1988, eleven agencies existed in Europe, of which seven were members of the European Community"). NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 96, 98.

[865] Newman, *supra*, at 112, 114.

[866] *Id.*, at 119-120, 122 (arguing that delegated agencies "derive their preferences from a variety of sources including professional training, ideological commitments, and a desire to maintain their authority").

[867] *Id.*, at 112-14 (noting that the transgovernmental network "met annually to debate pressing issues, share information, discuss best practices, and release joint resolutions on political matters"; and that DPAs "resolved in a 1989 meeting in Berlin that the European Community must take action on data privacy to guarantee the free flow of information within the Community," concluding "with a resolution demanding supranational action).

[868] *Id.*, at 113, 119. NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 98.

Dissatisfied with the *multilateral* treaty of the Convention 108, these actors started to orient the thrust of their efforts to negotiate norm-setting, rule-making, implementation, and enforcement through the European Union's *unilateral* acts,[869] pushing for a directive to supranationalize data privacy protection across Europe. Such a lawmaking dynamic is characterized by vertical forum-shifting from a multilateral venue to the unilateral legislative procedure at the Union level. Several major reasons account for this lawmaking strategy.

First, during the EU's legislative process, the network of national DPAs can utilize their asymmetrical powers to foist their preferences on the European Commission, which was primarily concerned with the realization of fundamental European projects (most notably, European market integration). By leveraging their newly acquired regulatory powers to block data exports, national data privacy commissioners (especially those from Germany and France) can alter the regulatory status quo for core supranational policymakers of inaction, and thus become crucial veto points to impede the realization of an internal European market. As will be detailed later, through high-profile regulatory actions, national data privacy commissioners threatened to obstruct free flows of personal data within the European market, pressuring the European Commission and several powerful member states to adopt their policy preferences for omnibus, strict data privacy throughout Europe. As such, successful integration of the European market was conditioned on ratcheting up the levels of data protection across Europe, producing an upward harmonization of national regulatory standards on data privacy protection.

Second, a legislation enacted by the European Union provides a more pragmatic and effective institutional route to achieve regulatory harmonization across Europe. Though a multilateral treaty, the Convention 108 only had a limited number of member states in the 1980s, and accession to it is quite politically challenging, for that requires a *unanimous* decision of contracting states representatives sitting on the Committee of Ministers.[870] In comparison, pursuing regulatory harmonization through the EU's unilateral legislation is more politically feasible. As amended by the 1987 Single European Act, directives and regulations enacted by the European Commission could be adopted by *a qualified majority* of the Council, only requiring the votes of 55% of member states representing at least 65% of the EU's population.[871] As such, the possibility to pass EU-wide legislation without consensus paves the way for ambitious regulatory agenda and robust rule-making.[872] Delegated with substantial powers to enact and implement measures necessary to create and maintain the single market, the Commission is empowered to use regulations to shape the European market and beyond, without the need to seek unanimity from the Council.[873] This makes the Commission a promising forum for national DPAs to push through their desired data privacy rules.

---

[869] As part of the sources of EU law, "unilateral acts" are the EU's secondary legislation adopted autonomously by EU institutions (the European Commission, Council, and Parliament), including directives and regulations. EUR-Lex, Unilateral Acts, March 21, 2018 https://eur-lex.europa.eu/EN/legal-content/summary/unilateral-acts.html#:~:text=What%20are%20unilateral%20acts%3F,accordance%20with%20the%20founding%20treaties.
[870] Convention 108, art. 23(1). See *supra* Part II.
[871] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 13 (2020). See The Single European Act, https://eur-lex.europa.eu/EN/legal-content/summary/the-single-european-act.html.
[872] *Id.*
[873] *Id.*, at 17.

When adopted by the European Union, a directive (or regulation) constitutes the EU's secondary law,[874] obliging all EU member states to enact domestic legislations to implement its provisions. Compared with relying on a multilateral treaty to gradually expand its membership, the enactment of an EU legislation provides a more effective and convenient route to harmonize regulatory standards within Europe. Further, there are important institutional safeguards to ensure member states' compliance with the EU's legislation. Within the EU's institutional framework, the European Commission is responsible to oversee implementation and enforcement of EU legislation: if any member state fails to implement a directive or regulation, the Commission has the authority to challenge that state before the ECJ to ensure compliance.[875]

Third, the network of national DPAs can use an EU directive to consolidate their delegated powers at both member state and the EU levels, strengthening their competence and authority to regulate data privacy protection. Discontented with the Convention 108 that has no specialized oversight institutions to ensure its implementation, national data privacy commissioners hoped to fill this gap through an EU directive. To that end, their preferred institutional solution was to make it compulsory in all member states to establish independent supervisory authorities mandated with similar advisory, regulatory, and oversight powers.[876] In addition, national DPAs also wanted to establish a new supranational institution composed of their representatives to formalize and solidify their transnational network, embedding these actors at core of the EU's policymaking process.[877] In this way, an EU directive can entrench the role of national DPAs not only as regulatory and law enforcement agencies to police data privacy in each member state, but also as politically powerful data privacy advocates at the supranational level.

In short, by shifting the rule-making processes to the EU level, national data privacy commissioners are enabled to play to their regulatory powers to control market access, mobilize important political support from the Commission and key member states, shape supranational data privacy lawmaking in ways that reflect their policy preferences, and secure Europe-wide data privacy rules that are difficult to make at the multilateral level. In other words, the lawmaking strategy of forum-shifting provides these powerful sub-state actors with an important institutional channel to reconfigure European data privacy framework based on their preferences and visions.

B. The Role of National DPAs as Norm Entrepreneurs Pushing the Commission to Enact a Supranational Regulation

By deploying their power resources (including technical expertise, regulatory and enforcement powers, and transnational network ties with each other), national DPAs managed to impose their preferences of EU-wide high-standard data privacy protection on the Commission, and substantially influenced the content of the legislative proposal eventually adopted.[878] This was the

---

[874] There are two sources of EU law: primary law and secondary law. The former refers to treaties laying down the legal framework of the EU (including the Treaty on European Union, and TFEU), and is the supreme source of EU law at the top of European legal order. The latter includes regulations, directives, decisions, as well as opinions and recommendations made by EU institutions. See E-Justice, EU Law, November 17, 2021, https://e-justice.europa.eu/content_eu_law-3-en.do.

[875] BRAFORD, *supra* (THE BRUSSELS EFFECT), at 9.

[876] See NEWMAN, *supra*, at 74-5, 97-8.

[877] See *Id*.

[878] *Id.*, at 97-8.

case, despite the initial reluctance of and opposition from the European Commission, key member states (such as the German, French, and British governments), and important business interest groups in the mid-1980s.[879]

(A) Building Issue-Linkages between Data Privacy Protection and Fundamental European Projects

Since the late 1980s, the transgovernmental network of national DPAs actively sought to mobilize political opinion, and lobby the Community, while framing the issue of supranational data privacy protection as a prerequisite to competing the internal market and administrative integration of Europe.[880] Using their expertise in this area, these transgovernment actors framed the underlying issues in ways to overcome potential objections to their proposals.[881] As such, the debate on data privacy protection was transformed from purely about civil liberties to the successful completion of politically salient European projects,[882] appealing to the Commission's prevalent concerns at the time.

(B) Leveraging Domestic Data Embargo Powers to Alter the Reversion Point

Moreover, national DPAs from powerful member states with high-standard data privacy laws leveraged their "data embargo" powers to change the regulatory status quo that would have existed without a supranational legislation, effectively altering the cost-benefit calculation of key European policymakers of inaction.[883] Deploying their regulatory authority to control market access, these DPAs threatened to unilaterally block data flows to countries without adequate data privacy protection levels, changing the reversion point for the Commission in case of no supranational regulation.[884] In this regard, two instances are particularly notable.

The first case concerns multinational companies' data transfers. In July 1989, the French national DPA (CNIL) invoked domestic data privacy law against Fiat, and threatened to ban transfers of personal data from Fiat's French offices to Italy, on the ground that Italy did not have adequate data privacy protection.[885] The resultant "data embargo" dilemma pressed Fiat Italy to make great concessions by signing a data privacy contract, undertaking to ensure that personal data transferred

[879] Newman, *supra*, at 110-12.
[880] Newman, *supra*, at 113-14 (noting that in a March 1990 conference, DPAs concluded "with an appeal to the European Community to pass a privacy directive to avoid data blockages and secure individual liberty within the emerging single market of the community").
[881] *Id*., at 121.
[882] *Id*.
[883] *Id*., at 114, 121.
[884] According to rational choice literature, the "reversion point" refers to "the character of the status quo in the absence of successful coordination" and "is a key factor influencing the bargaining strength of states". See Henry Farrell & Abraham Newman, *Making Global Markets: Historical Institutionalism in International Political Economy*, 17 REVIEW OF INTERNATIONAL POLITICAL ECONOMY 609, 625 (2010); John E. Richards, *Toward a Positive Theory of International Institutions: Regulating International Aviation Markets*, 53(1) INT'L ORGAN. 1, 13 (1999). Also known as "best alternative to no agreement (BATNA)", "reversion point" is an institutionally determined fallback point. "Parties with more favorable reversion points can drive harder bargains." See Susan Sell, *The Rise and Rule of a Trade-Based Strategy: Historical Institutionalism and the International Regulation of Intellectual Property*, 17 REVIEW OF INTERNATIONAL POLITICAL ECONOMY 762, 777 (2010).
[885] Journal Officiel de la République Française 1978. Loi No. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

from Fiat France are protected under French data privacy law.[886] Far from alone, this instance is emblematic of the regulatory actions launched by powerful DPAs at the time, which deployed their data embargo powers to press European countries without data privacy laws to pass such legislations.[887]

The other case relates to the Schengen project. In the late 1980s when France, Germany, Belgium, the Netherlands, and Luxembourg were negotiating a Schengen agreement (a regional border control agreement to permit the free movement of individuals among them), the French, German, and Luxembourg DPAs stepped in and blocked the deal from going further.[888] While the underlying agreement aimed to establish the Schengen Information System (which networked national custom and border control databases to mutually police national borders), Belgium at the time did not have a data privacy law, potentially serving as a regulatory loophole.[889] Concerned that sharing sensitive personal data with Belgium would breach their national data privacy laws, these DPAs threatened to ban the creation of a single European market for labor, and conditioned the conclusion of the Schengen agreement on a data protection solution.[890] Under such external pressures, Belgium promised to pass national data privacy legislation.[891] The political importance of the Schengen agreement to the Commission (which deemed it an essential first step toward achieving free movement of labor within the Community)[892] translated into potential costs for policymakers at the Community level in the absence of a supranational data protection regulation.

In short, by the end of 1980s, national DPAs of the most powerful member states in the Community—France and Germany—required stronger data privacy protection throughout Europe, backed by credible threats of data embargo against other member states with laxer or no data privacy rules.[893] In the multilevel governance system of the EU, political authority is concurrently distributed among numerous overlapping institutions, and successful completion of European internal market and administrative integration at the time demanded a high degree of cooperation of member states. These dynamics enabled national DPAs to wield regulatory authority previously confined to domestic settings at the European level,[894] amplifying their powers to influence the policymaking of the Commission. Leveraging their data embargo powers to control access to their large domestic markets, national DPAs in these powerful member states became *de facto* veto players in the negotiations of European trade liberation rules and other fundamental pan-European projects.[895] In this way, these actors had effectively altered the regulatory status quo for the Commission and EU member states that hoped to complete the single European market project.[896]

---

[886] Transnational Data and Communications Report, No Fiat for Fiat, November 1989, at 10.
[887] For instance, in September 1989, the CNIL also threatened to block transfer of sensitive medical personal data from a French medical research center to a European cancer research center located in Belgium for the latter's lack of national data privacy law. The CNIL required Belgium to enact data privacy legislation. See Newman, *supra*, at 115.
[888] Newman, *supra*, at 115.
[889] *Id.*
[890] *Id.* See Jacques Fauvet, *Transnational Data and Communications Report*, November 1989, at 17–18.
[891] Newman, *supra*, at 115.
[892] *Id.*
[893] See Shaffer, *supra* (Globalization *and Social Protection*), 12.
[894] Newman, *supra*, at 121-22.
[895] *Id.*
[896] *Id.*, at 116 (noting that one member of the Internal Market directorate in charge of drafting the DPD 95 expressly stated that "the Commission was held hostage by data privacy authority demands" and that these transgovernmental actors had successfully altered the reversion point, and hence, "used their domestically delegated authority to change

As a result, the Commission internalized the preference of these DPAs. Though it rejected a recommendation by the Parliament for passing a data protection directive in the early 1980s,[897] the Commission's attitude shifted considerably in the early 1990s, as it adopted the framing and policy solutions of national DPAs.[898] Realizing that impeded cross-border data flows within Europe threatened pan-European market integration (and hence, were within its jurisdiction),[899] the Commission responded by leveraging its agenda-setting powers to push forward a Union-level legislation—the EU Data Protection Directive 1995.

(C) Utilizing Expertise and Network Ties to Influence the Shape of the Directive

To find a supranational regulatory solution, the Commission set forth a drafting committee by the late 1980s, composed of Commission officials and representatives of national DPAs, to formulate the European Data Protection Directive.[900] As such, national DPAs had been vertically embedded into the international bargaining process at the Union level, and the Commission's officials heavily relied on their expertise to address complex issues of data privacy.[901] Also, national DPAs sat alongside many member-state representatives in the Council of Ministers meetings, and hence, can use their expertise to influence member states' positions and proposals, which proved crucial in overcoming the latter's concerns and reaching a political deal.[902] By leveraging their institutional expertise and vertical ties, national DPAs had amplified their capacity to pronounce their preferences and to control agenda formation during the rule-making process, which was instrumental to the progress of the Directive.[903] In this way, these actors have substantially influenced the content of the Directive. In comparison, little consultation was done with the private sector before the Commission's release of its proposal for a framework directive, and the business community had lost the agenda-setting initiatives to national DPAs.[904]

C. The EU Data Protection Directive of 1995

---

the preference calculation of actors at other levels), 118; BYGRAVE, *supra*, at 55 (noting that "[o]nly when faced with clear signs that the uneven nature of EU member states' respective (data privacy) rules… threatened … realization (of the internal market) did the Commission put serious effort into drafting a framework Directive").

[897] Newman, *supra*, at 110-11. See Commission Recommendation 1981 O.J. (L246), at 31.

[898] Newman, *supra*, at 116.

[899] Treaty Establishing the European Economic Community, March 25, 1957, art. 100 ["The EEC Treaty"]. Article 100 authorizes the Council, acting on a proposal of the Commission, and after consulting the Parliament, to enact a directive to approximate the "legislative and administrative provisions of the Member States" directly affecting the "establishment or functioning of the Common Market".

[900] Newman, *supra*, at 117 (noting that "[a] member of the CNIL was seconded to the Commission as a policy specialist and the Commission relied heavily on the advice of national data privacy officials").

[901] *Id.* (quoting the internal Market Commissioner John Mogg: "The Commission is in a learning process, ready to hear from those who have the experience, and first of all the Data Protection Commissioners"). See John Mogg, *Initiatives taken by the European Communities in the Field of Data Protection: New Developments*, Remarks presented at the 13th Conference of the Data Protection Commissioners, October 1991, Strasbourg, France.

[902] *Id.*, at 118, 123 (quoting Mogg: "In these negotiations the contribution of the European Data Protection Commissioners, where it existed, has been very helpful not only in clarifying and enriching the debate but in the finding of a final comprise" and that the German delegation appointed the German federal data privacy commissioner, Dr. Joachim Jacob, to represent the Germany presidency during the negotiations).

[903] *Id.*, at 123.

[904] *Id.*, at 117.

After more than five years of negotiations, the Directive was adopted by the EU in October 1995.[905] Driven by national DPAs as politically powerful privacy advocates, the Directive emerged from the convergence of interests between these independent regulatory agencies seeking to strengthen data privacy protection and defend their authority, on the one hand, and the Commission and member states which strived to achieve fundamental European projects, on the other hand.[906] By requiring an equivalent level of data privacy protection within Europe, the Directive addressed the threats of data embargo between member states.[907] To ensure European market integration and trade liberalization, EU member states collectively consented to implement a comprehensive and robust set of data privacy rules, manifesting an "upward harmonization" of regulatory standards.[908]

Incorporated into the 1992 Agreement on the European Economic Area (EEA), the Directive obliges 27 EU member states and 3 countries that are parties to the EEA Agreement (i.e., Norway, Liechtenstein, and Iceland) to implement its provisions through national legislations.[909] As a result, not only the five countries without data privacy legislations—Belgium, Italy, Greece, Spain, and Portugal—adopted such laws in the 1990s, but other member states were also required to revise their domestic data protection laws to comply with the Directive.[910]

(A) Conceptualizing The Right to Personal Data Protection as a Fundamental Right

While largely emerging from the economic concerns that divergent national data privacy regimes in Europe would prevent the realization of the internal market, the EU Directive sought to address this underlying challenge by ensuring high-standard data privacy protection across Europe. As stated in article 1, the EU Directive had twin objects: to protect natural persons' data privacy as "fundamental rights and freedoms", and to prevent member states from impeding the "free flow of personal data" between themselves for reasons of data privacy protection.[911] Though seemingly pointing in different directions, these two objectives were inseparable. Since "downward harmonization" was politically infeasible under the data embargo threats of national DPAs (especially those of Germany and France with large domestic markets), the Directive chose to ratchet up data privacy standards to ensure free data flows across Europe.[912]

Notably, the Directive explicitly recognized the fundamental right status of data privacy protection. Such a "fundamental right" conceptualization of data privacy protection followed the normative

[905] EU Data Privacy Directive, at 31.
[906] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 97-98.
[907] EU Data Protection Directive, preamble, paras. 7-9; Recital 8.
[908] Shaffer, *supra* ("*Globalization and Social Protection*"), at 11. BRAFORD, *supra* (BRUSSELS EFFECT), at 10-11.
[909] BYGRAVE, *supra* note, at 54.
[910] Newman, *supra*, at 118.
[911] See EU Data Protection Directive 95, art. 1; Recitals 3, 5, 7 (emphasizing a concern to achieve the internal market of the EU, whereby personal data, along with goods, services, capital, and persons, are able to freely flow between member states); and Recitals 2, 3, 10, 11 (stressing the importance of protection of basic human rights, including the right to privacy, in the context of computer technologies).
[912] See the previous sub-section; see also Shaffer, *supra*, at 11-13 (noting that EU "Member States' institutional approaches to data privacy protection were thus interdependent"); BYGRAVE, *supra* note, at 58 (arguing that "the Directive should not be viewed as merely constituting the lowest common denominator of rules found in member states' pre-existing laws").

trajectory of the Convention 108,[913] and was consistent with the recognition of a constitutional right to personal data protection in some member states with stringent data privacy laws (such as Germany).[914] While the Directive aimed to promote and facilitate transborder exchange of personal data within the Union, this policy goal was not to be pursued at the cost of high-standard data privacy protection across Europe.[915] The importance of fundamental rights in the Directive's agenda was subsequently recognized by the ECJ in several seminal judicial decisions.[916]

(B) High-Standard Regulatory Controls over Data Processing

Unlike the U.S. sectoral approach to data privacy protection, the EU Data Protection Directive exemplifies an omnibus regulatory approach, characterized by a relatively stringent set of rules. Using far more prescriptive language than Convention 108, the Directive specifies a high-standard baseline of data privacy protection.[917] Such a robust level of protection is achieved through the creation of ex ante and ex post regulatory controls over data processing and a set of individual rights conferred on data subjects.

First, by establishing a comprehensive framework to protect individuals' data privacy, the Directive covers all personal data processing in the public and private sectors.[918] While the U.S. approach uses narrowly tailored data privacy rules to regulate specific sectors and relies heavily on business self-regulation,[919] the Directive covers private sector processing of personal data in all areas of the economy. And, on top of the Directive, the EU further enacts sectoral laws to regulate special categories of data processing (such as that in the telecommunication sector).[920]

Second, the Directive imposes a relatively stringent set of regulatory standards on data controllers for the processing of personal data. Though its basic principles of data privacy protection are modelled on the Convention 108 and OECD Guidelines, the Directive is far more prescriptive in specifying the obligations of data controllers for data processing, and goes substantially further in defining the normative content of data protection.[921] In this sense, the Directive seeks not only to "give substance to", but also to "amplify" the data privacy principles provided in the Convention

---

[913] Convention 108, art. 1 ("The purpose of this convention is to secure… respect for… rights and fundamental freedoms, and in particular… right to privacy, with regard to automatic processing of personal data…"). See Bygrave, *supra* (Strasbourg Effect), at 7.

[914] For instance, German constitutional law recognized data privacy protection as a "right to informational self-determination" in 1983 and a "right of trust and integrity in information systems" in 2008, holding that data processing threatens individuals' decisional authority and personal integrity, as well as "a free democratic community based on its citizens' capacity to act and participate". See Schwartz and Peifer, *supra*, at 126-27; see also BVerfG, 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 (Volkszählungsurteil) (Census case), Dec. 15, 1983.

[915] Schwartz and Peifer, *supra*, at 131 ("Free flow of information matters, but not as much, ultimately, as the safeguarding of dignity, privacy, and data protection in the European rights regime"). Chander and Schwartz, *supra*, at 30.

[916] BYGRAVE, *supra*, at 58. See *infra* Section III.A.(A).

[917] BYGRAVE, *supra*, at 59.

[918] EU Data Protection Directive 95, art. 3 (the exceptions include matters of public security, defense, state security, criminal law, and "purely personal or household activity"). See BYGRAVE, *supra* (DATA PRIVACY LAW), at 62.

[919] Reidenberg, *supra* (*Resolving Conflicting*), 1331.

[920] DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 1096 (2015).

[921] BYGRAVE, *supra*, at 63.

108.[922] For instance, while reiterating the principle of data quality of the Convention 108,[923] the Directive is unique in explicitly prohibiting the processing of personal data unless specified conditions are satisfied.[924] On top of that, the processing of sensitive personal data is subject to even stricter requirements, such as the data subject's "explicit consent" to the processing.[925] As such, the processing of personal data under the Directive requires a legitimate basis provided thereunder, otherwise the operation constitutes a violation of the law in itself.

Further, the Directive requires data controllers to provide data subjects with the basic information to ensure fair processing (including the "identity of the controller" and its representative (if any), the "purpose of the processing", and the "recipients or categories of the recipients of the data"), independently of the data subjects' right to access.[926] Such an obligation even extends to scenarios whereby the data concerned have not been obtained from the data subject, though to a lesser extent.[927] The failure to expressly inform the data subject of such required particulars may invalidate the underlying consent for processing his data.[928]

Third, unlike the Convention 108 which does not create individual rights,[929] the Directive requires member states to establish a robust set of individual rights for data subjects, who are thus entitled to monitor and challenge the processing and use of their personal data. For example, the Directive provides individuals with a right of access. By invoking this right, a data subject may obtain from the data controller, without excessive delay or expense, copies of the data about him, confirmation about the purposes of the processing and the recipients or categories of recipients, and even "knowledge of the logic involved in any automatic processing of data concerning him."[930]

Further, the Directive grants individuals substantial enforcement rights to protect their data privacy. As required by the Directive, data subjects can request the data controllers to correct their personal data when those data are inaccurate or incomplete, and may even block further processing of that information.[931] Under the right to object, a data subject must "be informed before his personal data are disclosed for the first time to third parties… for the purposes of direct marketing," and may challenge such disclosures or uses free of charge.[932] The Directive also endows individuals with a novel, though qualified, right to challenge certain automatic decision-making processes that significantly affect them, where such decisions are solely based on automatic processing of their

[922] EU Data Protection Directive 95, Recital 11.
[923] EU Data Protection Directive 95, art. 6(1) (Principles relating to data quality); compare with Convention 108, art. 5 (Quality of data).
[924] *Id.*, art. 7 (these legal grounds include unambiguous consent, necessity for the performance of a contract, necessity for compliance with a legal obligation, necessity to protect the vital interests of the data subject, among others).
[925] *Id*., art. 8. Such an "explicit consent" requirement is stricter than the "unambiguous consent" condition for the processing of non-sensitive personal data. Compare with Id., art. 7(a).
[926] *Id.*, art. 10.
[927] *Id.*, art. 11.
[928] Shaffer, *supra* (*Globalization and Social Protection*), at 15.
[929] Explanatory Report on Convention 108, para. 38.
[930] EU Data Protection Directive 95, art. 12(a)(c).
[931] *Id.*, art. 12(b).
[932] *Id.*, art. 14(b).

personal data (such as those relating to their creditworthiness or work performance).[933] Finally, the Directive obliges member states to provide data subjects with the right to a judicial remedy for breaches of their individual rights, including the right to obtain damages (if any).[934]

Fourth, the Directive provides for extraterritorial application of the data protection law of a member state adopted to implement its provisions, though to a limited extent. Most notably, it requires the national data protection law of a member state to apply outside the EU, where a controller outside Europe utilizes equipment located within that state to process personal data.[935]

(C) Strong Controls over Cross-border Transfers of Personal Data

In terms of cross-border data flows, the Directive takes a layered approach to regulate this issue-area. For purposes of internal transfers within Europe, it disallows EU member states to restrict or prohibit free flow of personal data between themselves for the reason of data privacy protection.[936] By requiring member states to implement omnibus data protection laws featuring stringent regulatory standards, the Directive aims to remove internal barriers to personal data flows arising from divergent national regulations.

In contrast, the Directive adopts a qualified prohibition approach to regulate cross-border personal data flows to third countries. Under article 25, member states must disallow transfers of personal data to a country outside Europe, unless that country provides "an adequate level" of data privacy protection.[937] To reach such a decision, the Commission or a member state would look to a set of substantive requirements, including the extent to which a third country's legal system adheres to basic data privacy principles under EU law, as well as additional data privacy requirements (such as those for sensitive data, on direct marketing, and on automated decision-making).[938] For that purpose, the EU examines not only the content of data privacy principles provided under that foreign legal system, but also the effectiveness of these principles implemented by oversight, enforcement, and redress mechanisms.[939] As construed by the ECJ, "adequacy" means an "essentially equivalent" level of data privacy protection between the EU and the third country.[940] A such, unlike the Convention 108 that failed to regulate cross-border data flows to a non-

[933] *Id.*, art. 15 (a data subject has the right to not be subject to any decisions that significantly affects him, and which is "based solely on automatic processing of data", designed to evaluate his certain personal aspects—such as creditworthiness or work performance).
[934] *Id.*, arts. 22-23.
[935] *Id.*, art. 4(c) (the only exception is if "such equipment is used only for purposes of transit through the territory of the Community").
[936] *Id.*, art. 1(2).
[937] *Id.*, art. 25(1).
[938] KUNER, *supra*, at 65.
[939] Article 29 Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, DG XV D/5025/98, WP 12, July 24, 1998, at 6-7, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf; Yves Poullet and Serge Gutwirth, *The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of 'Reflective Governance'?*, 2008, at 15-16, https://www.academia.edu/27153946/The_contribution_of_the_Article_29_Working_Party_to_the_construction_of_a_harmonised_European_data_protection_system_an_illustration_of_reflexive_governance (describing a "double assessment").
[940] *Schrems I*, paras. 73, 74, 96; *Schrems II*, paras. 94, 105, 162.

contracting state, the "adequacy" standard under the Directive aims to prevent third countries from becoming "data havens" in circumvention of European data privacy rules.

The process leading to a finding of "adequacy" is complex and prolonged.[941] Only a handful of countries obtained such a decision under the Directive.[942] In the absence of such an "adequacy" status, the Directive provides two sets of institutional alternatives to transfer personal data.

First, the ban on cross-border data flows may be lifted, where the data controllers rely on enumerated grounds for derogations under article 26(1). These include the unambiguous consent of the data subject, necessity for the performance or conclusion of a contract, important public interest grounds, or the vital interests of the data subject.[943] But these derogations may only be utilized to a limited extent under relatively stringent conditions, are typically complex and cumbersome in practice, and in any event, cannot be used to undercut the "principle of adequate protection" as enshrined in article 25.[944] Thus, it is difficult to use those derogations for massive, repeated, or regular international data transfers without incurring substantial costs.

Second, the Directive also allows transfer of personal data outside Europe, if the data controllers provide "adequate safeguards" on data privacy protection in the form of "appropriate contractual clauses." [945] These "adequacy safeguards" primarily include two mechanisms of binding contractual commitments: the standard contractual clauses (SCCs) and binding corporate rules (BCRs). As European accountability mechanisms, these contractual arrangements allow the data controllers to voluntary follow pre-negotiated binding standards that meet an adequate level of protection to transfer personal data outside Europe.

The SCCs are a set of model contractual clauses that are formulated and pre-approved by the Commission to ensure "adequate" data protection.[946] By saving the labor of drafting contracts from scratch and then seeking the EU's approval, the SCCs simplify the process of writing personal data transfer agreements. In addition, the SCCs also allow *ad hoc* contractual clauses that depart from

---

[941] KUNER, *supra*, at 65 (outlining the steps that lead to an adequacy finding by the EU: "a formal request from the (applicant) country…; a proposal from the European Commission…; an opinion of the Article 29 Working Party; an opinion of the Article 31 Committee delivered by a qualified majority of the Member States; a 30-day period of scrutiny for the European Parliament…; an opinion adopted by the College of Commissioners").
[942] *Id.* (noting that the Commission only issued 13 adequacy decisions by 2013).
[943] EU Data Protection Directive, art. 26(1).
[944] See eg. Article 29 Working Party, Working Document on A Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, Adopted on November 25, 2005, at 11, 17, https://www.pdpjournals.com/docs/88080.pdf (stating that "consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question… Relying on consent may therefore prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome"). For restrictions on invoking other grounds of derogations, see id., at 13-16. KUNER, *supra*, at 43. Poullet and Gutwirth, *supra*, at 15 (noting that since article 25 of the Directive establishes an "adequacy" standard as a general principle, this requires a strict interpretation of the derogations provisions under article 26).
[945] EU Data Protection Directive, art. 26(2).
[946] Chander and Schwartz, *supra*, at 35. "Accountability mechanisms" allow companies to opt into established data privacy standards to protect international data transfers, making data operators "accountable" for their processing of personal data. As "a private alternative to broader legal mandates", privacy accountability mechanisms provide "an organizationally-based approach to transborder data transfers that private and public authorities then reinforce". See *id.*, at 6, 26, 33.

their "off-the-rack" language, yet those revised provisions must be approved by the local DPAs in the member state from which the data are to be transferred.[947]

The BCRs refer to a legally binding set of data processing rules adopted by a firm or a group of affiliated firms, whereby the organization(s) promise to adhere to certain data privacy principles, grant rights to the data subjects, and cooperate with national DPAs, regardless of the geographic location of the processing activities.[948] Unlike the SCCs, there is no official model for the BCRs; rather, they are custom-drafted contractual commitments approved by the relevant DPA(s).[949] Through the BCRs, personal data can be transferred from the EU to a country without an adequacy decision, but only within the entire corporate group (from one corporate member to another), which are deemed a "safe haven" with the same level of protection.[950]

While the EU recognizes these accountability mechanisms as legitimate grounds to transfer personal data to a third country without an "adequacy" decision, the SCCs and BCRs are by no means lenient instruments that would water down the EU's level of data protection. Unlike the US-promoted model of the APEC CBPR mechanism to transfer personal data across national borders, these EU accountability mechanisms are designed to provide relatively stringent data privacy commitments, prioritizing the value of privacy over the economic interests of trade.[951]

First, the SCCs and BCRs are, in essence, a contractual embodiment of the rigorous European data privacy standards, incorporating the legal protections based on EU law. By design, accountability mechanisms require the original collector of personal data to comply with certain data privacy principles governing the initial data collection and processing, regardless of the geographical location of the data processing.[952] But those principles (on which data protection is based) vary significantly under different accountability mechanisms.[953] In case of the U.S. model, the APEC CBPR system is designed to implement the APEC Privacy Framework, characterized by a relatively lower set of data privacy standards, "a mild prescriptive bite", and broad exceptions.[954] In contrast, the SCCs and BCRs oblige data controllers to remain accountable for compliance with core European data privacy principles featuring relatively stringent standards.[955]

For instance, unlike the APEC Privacy Framework that remains silent on this matter, European data protection law regulates "onward transfers": namely, further transfers of personal data from the initial third country of import.[956] Under the Directive, as is the initial transfers, "onward transfers" should be permitted only if the second recipient country provides an adequate level of data protection, with the only exception being the derogations and accountability mechanisms

[947] *Id*. KUNER, *supra*, at 43.
[948] Chander and Schwartz, *supra*, at 35.
[949] *Id*., at 36 (noting that "there is no official template, but only guidance as to the necessary internal corporate rules", and that for this reason, implementing BCRs creates greater administrative burdens than SCCs).
[950] *Id*., at 35. KUNER, *supra*, at 43-44.
[951] Chander and Schwartz, *supra*, at 36.
[952] KUNER, *supra*, at 71-72.
[953] *Id*.
[954] BYGRAVE, *supra*, at 76.
[955] KUNER, *supra*, at 71-72.
[956] KUNER, *supra*, at 44.

provided in article 26.[957] However, given the complexity involved in "onward transfers", the SCCs used for that purpose need to be tailor-made and would become highly intricate, generating considerable compliance burdens and legal costs for individual firms.[958]

Second, the U.S. and EU models of accountability mechanisms also differ in their oversight and enforcement authorities. Under the APEC CBPR, the U.S. relies on a combination of private sector accountability agents (TrustArc (formerly TRUSTe)) and governmental agencies (Federal Trade Commission (FTC)); but overall, enforcement actions thus far are rather limited in number, and less intense in terms of the sanctions imposed.[959] In comparison, the SCCs and BCRs are enforced by an array of European regulatory, legal, and constitutional institutions mandated to safeguard individuals' data privacy protection. In the first instance, these contractual mechanisms are policed by independent supervisory institutions established to implement the Directive—national DPAs.[960] Eager to implement, promote, and enhance data privacy, these authorities are known for their active enforcement actions and robust sanctioning powers. Further, as will be detailed later, after data privacy protection has been constitutionalized in the EU, these European accountability mechanisms are embedded into European constitutional framework, as they are meant to provide "adequate safeguards" for personal data and privacy protection as fundamental rights.[961] This means that the SCCs and BCRs can be scrutinized by national courts and the ECJ for their compliance with European constitutional requirements.[962]

Third, the SCCs and BCRs are relatively costly and inflexible contractual mechanisms, creating substantial compliance costs and administrative burdens (especially for small and medium businesses).[963] The SCCs must be signed by the data exporter and data exporter for each data transfer, and are widely regarded as setting relatively onerous terms that can result in high administrative costs.[964] As for the BCRs, the approval process can be lengthy (and sometimes unpredictable regarding the outcome), and their implementation may be relatively "expensive and difficult for all but large multinationals".[965]

---

[957] *Id.* (quoting the Article 29 Working Group).
[958] LOTHARD DETERMANN, DETERMANN'S FILED GUIDE TO DATA PRIVACY LAW 41, 45 (4th ed. 2020) (noting that SCCs would become highly complex, in case of "onward transfer", such as that involving "external service providers, business partners, [and] government agencies (e.g. in case of investigations, litigation or reporting obligations)"; and that it "can be difficult or impossible" for the initial data exporter to use SCC terms verbatim for the "onward transfer").
[959] Andrei Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (January 3, 2019), https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview (noting that "during an almost two-year period, Truste reported 55 complaints, all of them resolved and none referred to the FTC. In fact, during the CBPR's existence there is no evidence of a company losing its CBPR certification; the only enforcement actions taken by the FTC were against three companies falsely claiming to be CBPR certified.").
[960] Chander and Schwartz, *supra*, at 36.
[961] See *infra* Part. III.A.(B); Part IV.B(B).
[962] *Id.* Chander and Schwartz, *supra*, at 36.
[963] Paul Schwartz, *Global Data Privacy: The EU Way*, 94 NEW YORK UNIVERSITY LAW REVIEW 771, 794 (2019) ["The EU Way"].
[964] FRANCESCA CASALINI & LÓPEZ GONZÁLEZ, TRADE AND CROSS-BORDER DATA FLOWS 20 (OECD Trade Policy Papers No. 220, 2019).
[965] *Id.* KUNER, *supra*, at 220.

(D) Establishing Independent Supervisory Authorities and Institutionalizing Their Transgovernmental Network

In addition to these substantive aspects, the Directive has also required institutional reforms in EU member states, consolidating national DPAs' regulatory authority at the member state level and their transgovernmental network at the EU level.

First, the Directive obliges each member state to establish independent supervisory authorities mandated to monitor, implement, and enforce national data privacy laws adopted pursuant to its provisions.[966] Prior to the Directive, many EU member states did not have national DPAs; and even among existing DPAs, the distribution of regulatory authority was not even, with some agencies having only limited enforcement powers.[967] Under the Directive, member states are legally required to create national DPAs, ensure a high degree of independence of these regulatory agencies (by buffering them from direct political control), and enhance their regulatory authority to implement and enforce domestic data protection laws.[968] In particular, the Directive demands national governments to endow these agencies with the powers to investigate and sanction (including the authority to block, erase, destruct personal data, and to impose a temporary or definitive ban on data processing),[969] equalizing their regulatory authority across different member states.

Second, the Directive also creates a new standing advisory body mainly composed of national and European DPAs—the Article 29 Working Party ("WP29")—thus institutionalizing national DPAs' transgovernmental network and vertical ties with the Commission's policymaking process.[970] Under the Directive, this working party is granted the powers to advise the Commission on data protection issues (including any proposed amendments of the Directive), evaluate the levels of data protection in the EU and third countries, assist the implementation of the Directive, and promote the harmonization of its enforcement.[971] The creation of this group has turned the relatively informal cooperation among national DPAs in the 1980s into a robust set of institutionalized transnational regulatory network.[972] Sharing a common perspective, national DPAs and the WP29 behave like a collective actor, continuously seeking to improve their oversight, enforcement, cooperation, and influence.[973]

---

[966] EU Data Protection Directive, art. 28.
[967] Newman, *supra*, at 112 ("By the end of 1988, eleven (data protection authorities) existed in Europe"). For instance, in the late 1980s, unlike German and France data protection authorities equipped with strong data embargo powers, their Luxembourg peers had only weak domestic authority to regulate market access. id, at 123.
[968] EU Data Protection Directive, art. 28.
[969] *Id.*
[970] *Id.*, art. 29.
[971] *Id.*, art. 30.
[972] NEWMAN, *supra*, at 95 ("The Working Party has a secretariat in Brussels that is funded and staffed by the Commission. It is chaired by one of the national data privacy authorities and also include the European data protection supervisor and a representative of the Commission. It meets five times per year and has some fifteen subgroups working on a number of specific regulatory issues…. The Working Party has published eight annual reports and over one hundred documents and has developed annual work plans in which it spells out its priorities for the year").
[973] Moritz Laurer & Timo Seidl, *Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation*, 13 POLICY & INTERNET 1, 7 (2021). David Barnard-Wills et al., *Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU*, 32 COMPUTER LAW & SECURITY REVIEW 587 (2016).

Notably, with the powers to issue opinions on EU data protection concerns to the Commission, the WP29 can wield substantial supranational influence by rendering authoritative (though technically non-binding) interpretations of the Directive and EU data privacy law. Not only do national courts and regulators routinely refer to this group's interpretations and advice regarding the Directive, but also many digital and technological companies (including multinational corporations) carefully follow its opinions and recommendations to change their data governance policies and business practices, in order to avoid legal uncertainties arising under EU law.[974]

Moreover, the establishment of the working party has also created the institutional space within the EU's policy feedback loop for national DPAs to meet regularly, develop a long-term agenda, and advocate for new regulatory initiatives on data protection regulation.[975] In this sense, the Directive has "officially installed a kind of 'privacy lobby group' at the heart of the European institutions."[976] Representing an elite epistemic community that believes in data privacy protection in Europe and across the world, the WP29 is formally embedded into the core data privacy policy-making process at the EU level.[977] By solidifying their transgovernmental network and vertical ties, the WP29 strengthens the effectiveness and authority of national DPAs in supranational data privacy governance.

In sum, different from the Convention 108, the Directive uses more prescriptive language to specify relatively stringent controls on the processing of personal data, confers robust individual rights on data subjects, establishes independent supervisory authorities with enhanced regulatory authority, and consolidates their transgovernmental network. Further, the Directive adopts a qualified prohibition approach to regulate international transfers of personal data: transfers outside the EU are allowed, *only if* the recipient jurisdiction achieves an "adequate" level of data protection. Such an "adequacy" standard is drastically different from that of the Convention, which generally requires free data flows between contracting states, but confers national regulators discretionary powers to restrict or ban them in limited circumstances. While the Directive also establishes accountability mechanisms as an institutional alternative to a country-based "adequacy" decision, these instruments (i.e., SCCs and BCRs) impose relatively stringent data privacy standards on companies, serving as a contractual extension of EU data privacy law.

III. VERTICAL FORUM-SHIFTING 2.0: CONSTITUTIONALIZATION OF DATA PRIVACY PROTECTION AND THE GDPR

While the EU Data Protection Directive was acclaimed as a major achievement in supranationalizing data protection across Europe, in the years since, institutional advocates for data privacy and human rights did not end their rule-making efforts there, but further pushed their agenda through the EU's lawmaking processes. This Part reviews the second lawmaking process, where a set of data-privacy-oriented institutional actors sought to enshrine data privacy protection into European constitutional framework (Section A), and to push through the GDPR to reform the

[974] NEWMAN, *supra*, at 95 ("As the representative of an international telecommunications company explained, clients read the opinions of the Working Party and ask service providers to meet their requirements. Notably, Google agreed to alter its data retention policy to comply with the wishes of the Working Party"). See *id.*, at 118-21.
[975] Laurer and Seidl, *supra*, at 95-96.
[976] Poullet and Gutwirth, *supra*, at 2.
[977] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 95-96.

Directive (Section B). Treating the Directive as a beginning (rather than an endpoint), such lawmaking initiatives have substantially developed and revamped EU data privacy regime, orienting it towards higher standards of data privacy protection.

A. Vertical Forum-Shifting 2.1: Constitutionalization of the Rights to Personal Data Privacy Protection and Privacy

After the EU regulated data privacy protection through EU secondary law (i.e., the EU Data Protection Directive), personal data and privacy protection underwent a process of "constitutionalization", and were consequently elevated to fundamental rights in European constitutional order. This institutional change not only created important normative implications for the application of data privacy rules, but also paved the way for the Commission to reform existing EU data protection framework.

(A) Anchoring Personal Data and Privacy Protection into European Constitutional Framework

Before getting to the dynamics of the "constitutionalization" process, it is worth noting two different, yet interrelated, Europe-wide constitutional sources of fundamental rights. The first is the 2000 Charter of Fundamental Rights of the European Union (the "EU Charter"). Originally, the EU Charter was a political instrument designed to recognize a set of national and international obligations.[978] Yet, with the Lisbon Treaty's entry into force in 2009, it became the EU's primary law legally binding on all EU member states.[979] Interpreted by the ECJ (the judicial body of the EU), the EU Charter is a pillar of fundamental rights for the EU's legal regime.[980] The second source is the ECHR, which was drafted by the CoE in 1953 and interpreted by the ECtHR. While the CoE is not a body of the EU but an independent international organization, all EU member states are parties to the ECHR, and thus bound by the rulings of the ECtHR.[981] This enables the ECJ to interpret the ECtHR jurisprudence covering the same sets of fundamental rights "as a legal floor in this space, technically not binding on the court itself, but binding on all of the Member States to which the [ECJ]'s rulings also apply."[982]

After the EU Data Protection Directive established a comprehensive regulatory framework governing the processing of personal data, the rights to personal data protection and privacy were anchored into the EU's constitutional order by the late 2010s, attaining the status of fundamental rights under EU primary law.

In 2000, the EU Charter explicitly recognized protection of personal data as an autonomous fundamental right (in article 8), independent of the right to privacy (in article 7).[983] In addition, article 8 reiterated key elements of fair information practices, including "(1) a requirement of fair

[978] Jones and Kaminski, *supra*, 102.
[979] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, signed on December 13, 2007, effective on December 1, 2009, 2007 O.J. (C 306) 13, art. 6(1) ["Lisbon Treaty"].
[980] Jones and Kaminski, *supra*, at 102.
[981] *Id.*, at 102-3.
[982] *Id.*, at 103.
[983] EU Charter, arts. 7, 8(1). See Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 125 (2017) ("With the signing of the Lisbon Treaty by EU member states, the Charter became binding constitutional law for the EU in 2009").

processing; (2) a requirement of processing for specified purposes; (3) a requirement of consent or other legitimate basis for processing; (4) a right of access to data; (5) a right to have data rectified; and (6) a requirement of independent data protection authorities checking compliance with these rules."[984] This provision reflects and incorporates the core components of many existing data protection laws, including the Convention 108, the EU Data Protection Directive, and some national data protection laws.[985]

Unlike the right to privacy that largely focuses on the protection of sensitive data, the right to personal data protection aims at restoring the power balance between data operators and data subjects.[986] To that end, this right disciplines data processing activities, ensures individual rights of data subjects to control their data, and focuses on the requirements of fair processing, transparency, consent, and legitimacy, which cannot be adequately dealt with by the "right to privacy".[987] Further, this provision confers a constitutional status to the rights to data protection and privacy, and thus establishes the primacy of data privacy over competing economic or security interests implicated in data processing.[988] In addition, by virtue of this provision, the role of DPAs has gained "constitutional" importance.[989]

As amended by the 2009 Lisbon Treaty, the right to personal data protection (including these core data protection principles) under the EU Charter became part of EU primary law, obliging all the EU institutions and member states to comply with such constitutional requirements.[990] The Lisbon Treaty further constitutionalized data protection through the Treaty on the Functioning of the European Union (TFEU), which explicitly provided the right to personal data protection in article 16.[991] Under this provision, the European Parliament and Council are mandated to establish data protection rules to regulate the processing of personal data by the EU institutions and by member states (when acting under EU law).[992]

Two notable sets of institutions served as the major actors driving this constitutionalization process. First, the WP29 had played an important role in anchoring the right to personal data protection as an independent fundamental right in the EU Charter.[993] In 1999, the WP29 released an official

---

[984] Schwartz & Peifer, *supra* note, 128. See EU Charter of Fundamental Rights, art. 8(2)-(3).
[985] Jones and Kaminski, *supra*, at 103.
[986] Poullet and Gutwirth, *supra*, at 14.
[987] *Id*., at 15.
[988] Article 29 Working Party, Fifth Annual Report of the Article 29 Working Party, Adopted on March 6, 2002, 10557/02/EN final WP54, at 5. https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2002/wp54_2_en.pdf (noting that under this provision, "personal data protection cannot be considered solely and/or prevailingly in economic terms, nor may it be overridden by—albeit important—security requirements") ["WP29's Fifth Annual Report"].
[989] *Id.*
[990] Lisbon Treaty, art. 6(1).
[991] TFEU, art. 16 (1).
[992] *Id.*, art. 16(2). Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INTERNATIONAL DATA PRIVACY LAW 119, 123 (2012) (arguing that "the expression 'within the scope of Union law' must be interpreted as excluding only those areas which do not fall within the competences of the Union") ["*European Data Protection Framework*"].
[993] WP29's Fifth Annual Report, *supra*, at 5 (stating that article 8 of the EU Charter was "a major contribution" that "came from the activity carried out by the (WP29) in the past few years"); Article 29 Working Party, Seventh Annual Report of the Article 29 Working Party, Adopted on June 21, 2004, at 7, https://ec.europa.eu/justice/article-29/documentation/annual-report/files/2004/7th_report_prot_individs_en.pdf; Laurer and Seidl, *supra*, at 265.

recommendation, calling for the inclusion of the fundamental right to personal data protection in the European catalogue of fundamental rights.[994] Noting that the European Council decided to draw up the EU's Charter of Fundamental Rights, the WP 29 recommended the Commission, the Parliament, and the Council to incorporate the fundamental right to personal data protection into the Charter, and offered to help for drafting the Charter.[995] Stefano Rodotà, the chairman of the WP29, sat in the drafting committee, and was widely considered as one of the most important authors of the Charter,[996] with an indispensable role in adopting article 8 thereof.[997]

Moreover, the WP29 had influenced the drafting of the Draft Constitution for Europe.[998] Not only did the Draft Constitution incorporate the fundamental rights under the EU Charter (including article 8), but it also created an independent provision on personal data protection in article 50.[999] While the Draft Constitution was not eventually ratified, the succeeding TFEU adopted this latter provision in article 16.[1000]

The second set of actors is Europe's top-level judicial institutions—the ECJ and ECtHR. Through their jurisprudence, these two prominent courts of Europe have affirmed and developed the right to personal data protection.[1001] As held by the ECJ, the EU Data Protection Directive has protection of fundamental human rights as one of its primary goals, in addition to the purely economic concerns of European market integration.[1002] It also ruled that interpretation of the Directive shall partly turn on the interpretation of the ECHR by the ECtHR.[1003]

In parallel, prior to the EU Charter, the ECtHR has broadly interpreted the right to privacy under the ECHR beyond the traditional private sphere,[1004] transforming this right from a "privacy-intimacy" notion to a "privacy-self-determination" one.[1005] Before 2000, the ECtHR, influenced

---

[994] Article 29 Working Party, Recommendation 4/99, 5143/99/EN WP26, September 7, 1999, at 2-3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf ["WP29's Recommendation 4/99"].

[995] *Id*., at 3 (arguing that inclusion of this fundamental right would make data protection "a legal requirement throughout the Union and reflect its increasing importance in the information society").

[996] Sam Pfeifle, *Stefano Rodotà, Former Garante President and WP29 Chair, 1933—2017*, THE PRIVACY ADVISOR (July 19, 2017), https://iapp.org/news/a/stefano-rodota-former-garante-president-and-wp29-chair-1933-2017/; *Speech by the President of the Italian Data Protection Authority Presenting the 2005 Annual Report to Parliament—July 7, 2006*, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1332401.

[997] Poullet and Gutwirth, *supra*, at 14 (fn.57).

[998] Laurer and Seidl, *supra*, at 265.

[999] Draft Treaty Establishing a Constitution for Europe, July 18, 2003, 2003/C 169/20, Part I, art. 7(1) (Fundamental Rights), art. 50 (Protection of Personal Data); Part II (EU Charter), art. 8 (Protection of Personal Data).

[1000] TFEU, art. 16, compare with *id.*, art. 50. See Laurer and Seidl, *supra*, at 265.

[1001] See Juliane Kokott and Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INTERNATIONAL DATA PRIVACY LAW 222 (2013).

[1002] Joined Cases C-465/00, C-138/01, and C-139/01 *Rechnungshof v Österreichischer Rundfunk and Others* [2003] ECR I-4989 paras 39–45, 71ff.

[1003] See e.g. Case C-101/01 Bodil Lindqvist [2003] ECR I-12971; Case C-70/10 Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECR I-0000.

[1004] Jones and Kaminski, *supra*, at 104.

[1005] Poullet and Gutwirth, *supra*, at 14 (noting that the "privacy-self-determination" is defined as the right of a natural person to make his own choices in the society with respect to his personal data). See Gloria González Fuster & Serge Gutwirth, *Opening up Personal Data Protection: A Conceptual Controversy*, 29 COMPUTER LAW & SECURITY REVIEW 531, 536 (2013) (noting that the new privacy concept was largely described as offensive, while the old privacy notion was originally strictly defensive).

by the rise of EU data protection laws over time, had interpreted the right to privacy more broadly, and came to include personal data protection as an important aspect.[1006] While the ECHR does not explicitly provide for a right to personal data protection,[1007] the "changing case law of the (ECtHR)… has been progressively incorporating elements of data protection (as established in Convention 108) in its construal of the content of (the right to privacy) of the ECHR."[1008] In this way, the ECtHR has applied the right to privacy under the ECHR to give rise to a right to personal data protection. When drafting the EU Charter, the WP29 built on this development, and pushed through the inclusion of a fundamental right to personal data protection in the Charter.[1009]

(B) The Normative and Policy Implications of Constitutionalizing Data Privacy Protection

Within the EU's constitutional framework, protection of personal data has been enshrined as an independent fundamental right along with the right to privacy, making data privacy a higher value than the economic interests underlying personal data. Having the status of fundamental rights generates three major normative and policy implications for data privacy protection in Europe.

First, it bolsters the normative status of data privacy protection in the EU legal system, reinforcing the level of protection provided by EU law.[1010] Since data privacy protection is entrenched into European primary law, the rights to data protection and privacy then enjoy the same legal status as EU treaties, and constitute part of constitutional rights and general principles of EU law.[1011] Data subjects thus become privileged bearers of fundamental rights, rather than ordinary consumers in the marketplace. Such an elevated legal status makes breaches of data privacy more readily sanctionable. For example, under EU law, the fundamental rights of an individual may be interfered, even in the absence of sensitive data involved or any harm suffered by that person.[1012]

Further, the legal nature of fundamental rights makes derogations from basic data privacy norms more difficult. Under the EU Charter, any limitations of the fundamental rights "must be provided for by law" and "respect the essence of those rights", and shall satisfy the principle of proportionality.[1013] In the EU's constitutional system, it is the European judiciary's role to safeguard the essence of the fundamental rights under the Charter.[1014] In this regard, the ECJ has been increasingly stringent when applying the principle of proportionality to scrutinize data-processing activities.[1015]

[1006] Jones and Kaminski, *supra*, at 104; Fuster & Gutwirth, *supra*, at 536. See e.g., ECtHR, Amann v Switzerland, no. 27798/95, ECHR 2000-II, para. 65, Rotaru v Romania [GC] App no. 28341/95, ECHR 2000-V, para. 43.
[1007] ECHR, art. 8.
[1008] González Fuster & Gutwirth, *supra*, at 536.
[1009] WP29's Recommendation 4/99, at 2 (noting the ECtHR "have developed and defined a fundamental right based on various human rights which relate to the protection of personal data"); Poullet and Gutwirth, *supra*, at 14.
[1010] BYGRAVE, *supra* note, 59 (noting such a trend from the recent developments of ECJ jurisprudence).
[1011] Schwartz and Peifer, *supra*, at 126-27. KUNER, *supra*, at 62.
[1012] Schwartz and Peifer, *supra*, at 127. See eg. *Google Spain*, 2014 E.C.R. 317, para. 96; *Schrems I*, *supra*, para. 87.
[1013] EU Charter, art. 52(1).
[1014] Schwartz and Peifer, *supra*, at 129.
[1015] BYGRAVE, *supra* note, at 59; Schwartz and Peifer, *supra*, at 131 (noting that while the fundamental right of data privacy protection should be balanced with other competing interests in case of a conflict, any interference with the former should be pursued at the least constitutional costs, and that free flow of data matters not so much as protection of data privacy).

Moreover, the European fundamental rights of personal data protection and privacy create both a negative obligation and a positive duty for the governments to fulfill. As is the right to privacy in US law,[1016] these European fundamental rights provide constitutional safeguards for individuals against the intrusion of public powers, obliging public actors not to infringe on individuals' data privacy.[1017] Meanwhile, they also entail a *positive* duty for the EU and member states to enact and implement an effective legal framework to ensure robust protection of data privacy against private- and public-sector actors.[1018]

Second, the fundamental right to personal data protection provides the EU with a new legal basis to directly regulate data processing activities through comprehensive EU legislation.[1019] Previously, the competence of the EU to enact European data protection law emanated from the internal market legal basis, which justified insofar as using a non-self-executing *directive* to "approximate" national data privacy laws to ensure free flow of data across Europe.[1020] Namely, to the extent that divergent domestic regulations of member states may obstruct free movement of personal data flows within the EU, the European common market would be affected, justifying a directive under article 100 of the Treaty Establishing the European Economic Community ("the EEC Treaty") to assimilate or bring into closer alignment national laws on this matter.[1021] In contrast, under the Lisbon Treaty, the EU was conferred with a standalone legal basis to pursue EU-wide *regulation directly applicable* to all processing of personal data in the private and public sectors.[1022]

Further, the constitutional basis of data privacy protection situates data protection law into the European human rights backstop, mandating the ECJ to safeguard the protection of personal data and privacy at the EU and member state level. Notably, it grants the ECJ with the explicit authority to scrutinize and evaluate whether the laws, instruments, and practices of the EU institutions and member states (when acting under EU law) are adequately protective of the fundamental rights to data protection and privacy.[1023] This means that this Court may someday intervene as a final arbiter of EU law, finding the requirements or particulars of EU data protection law or member states' implementation of them violative of Europeans' fundamental rights. As noted by Chander and Schwartz, "[d]ata privacy has a normative backstop of an explicit constitutional status in the

[1016] Jones and Kaminski, *supra*, at 103 (noting that "in the United States, privacy is understood to create a barrier between the state and individuals, and otherwise enables individual autonomy" and "is largely invoked to require the state… to stop intrusions into the private sphere").
[1017] *Id.*
[1018] EU Charter, art. 8; TFEU, art. 16(2). See Mira Burri & Rahel Schär, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. PLCY. 479, 481 (2016). On the positive obligation of a fundamental right under the ECHR, see ECtHR, *Refah Partisi (The Welfare Party) and others v. Turkey*, App Nos. 41340/98, 41342/98, 41343/98, and 41344/98, Grand chamber judgment of February 13, 2003.
[1019] Reding, *supra* (European Data Protection Framework), at 120. See TFEU, art. 16.
[1020] Jones and Kaminski, *supra*, at 104 fn.59.
[1021] The EEC Treaty, art. 100. Evans, *supra*, at 576-77.
[1022] Article 29 Data Protection Working Party, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, Adopted on December 1, 2009, at 5 (such competence even extends to the processing of personal data in the areas of police and judicial cooperation in criminal matters as well as common foreign and security policy), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf ["The Future of Privacy"].
[1023] Jones and Kaminski, *supra*, at 103.

European Union, and an institutional backstop in the form of a high court, the [ECJ], eager to promote and enhance it."[1024]

Relatedly, the constitutionalization of data privacy protection creates an institutional incentive for multiple sets of partially overlapping regulatory institutions and judicial bodies in Europe to maintain, reinforce, and expand the interpretation and application of the fundamental rights to data protection and privacy. In the EU's constitutional system, there are a plurality of national and transnational judicial bodies and regulatory agencies mandated to protect human rights, often featuring "mutual influences and virtuous competition" in their interpretation and application of these legal sources.[1025] This institutional overlap creates "an incentive for an expansion of the norms and institutions for the protection of fundamental rights" from one level of the European multilevel system to other layers.[1026] For instance, when deciding cases on data privacy, the ECtHR's interpretations of the ECHR may later influence those of the ECJ, producing a legal feedback loop oriented towards stronger safeguards of fundamental rights.[1027] Also, as will be detailed later, the vigorous enforcement of fundamental rights by the ECJ could prompt national DPAs to more aggressively police cross-border transfers of personal data, ratcheting up the level of data privacy protection across Europe.

Third, anchoring data privacy protection into European constitutional law also changes the institutional dynamics within the Commission, paving the way for subsequent legal reform of EU data protection law. Given the strong precedent created by the EU Data Protection Directive, the constitutionalization of personal data protection makes it even more difficult for the Commission to water down the legal status quo, but incentivizes it to adopt legislative actions to strengthen data privacy, in order to give effect to the EU Charter and Lisbon Treaty.[1028] Since the Commission is bound to ensure the legal consistency of European legislative acts with EU primary law, the constitutional underpinnings of personal data protection constrain the Union's legislative leeway, and makes it more politically plausible for rights-oriented institutional actors within the Commission to push for a new reform of the existing EU data protection law.

B. Vertical Forum-Shifting 2.2: Reforming the EU Directive through the GDPR

In this lawmaking process, a coalition of institutional data privacy advocates has successfully transformed the EU Data Protection Directive into the GDPR. While these efforts originated from the need to update existing rules with technological advances and address a lack of harmonization among national laws, a group of rights-oriented institutions (most notably, the DG Just and WP29) has played an important role in shaping the policy agenda-setting as well as the drafting and adoption of the GDPR, explaining the timing, nature, and content of the regulatory reform. As a result, the Directive was replaced by a new regulation that further ratchets up the level of data protection and strengthens the regulation over cross-border personal data flows.

[1024] Chander and Schwartz, *supra*, at 31.
[1025] Schwartz and Peifer, *supra*, at 125; FEDERICO FABBRINI, FUNDAMENTAL RIGHTS IN EUROPE 13-14 (2014).
[1026] FABBRINI, *supra*, at 13.
[1027] Jones and Kaminski, *supra*, at 105.
[1028] See Laurer and Seidl, *supra*, at 5; MIRIAM HARTLAPP, JULIA METZ, AND CHRISTIAN RAUH, WHICH POLICY FOR EUROPE? POWER AND CONFLICT INSIDE THE EUROPEAN COMMISSION 18-20 (2014).

(A) The Institutional and Political Economic Dynamics underlying the GDPR

(a) New Challenges for Protecting Europeans' Personal Data

While the EU Data Protection Directive's principles remain valid still today, rapid technological developments and increasingly globalized flows of cross-border personal data brought new challenges for data privacy protection in Europe. Since the mid-2000s, there was an increasingly widespread use of social networking software, cloud computing, and automatic data collection enabled by the Internet-of-things (e.g., mobile Internet devices), generating new ways of creating, storing, using, and transferring personal information.[1029] Meanwhile, methods of data collection have become increasingly elaborated and less easily detectable, enabling private firms and public authorities to control an unprecedented amount of personal data. As a result, the risks of individuals losing control over their data (especially sensitive information) were on the rise, potentially undermining the level of protection enjoyed by European citizens.[1030]

In addition, technological advancements and deepened globalization add to the complexity surrounding the processing of personal data. Through the Internet, a growing number of non-EU-based data controllers and processors have been providing digital services to Europeans, and it is often difficult to determine the location of the data processed and of the equipment used—especially when data are stored or processed "in the cloud" (i.e. remote servers).[1031] Also, as digital firms were increasingly operating in several member states and/or third country jurisdictions, it is not always clear under the Directive which member state's law should be applied.[1032] With increased complexity as such, it is more challenging to ensure sufficient protection of Europeans' fundamental rights.

Moreover, the Directive, though a milestone in Europe's personal data protection, still left significant disparities among member states' domestic data protection laws and enforcement policies. This is due to its numerous textual ambiguities, as well as the exemptions and derogations allowed under this legislation.[1033] Consequently, member states' implementation resulted in considerable differences in their national legal approaches to data privacy protection and cross-border personal data flows.[1034] Such regulatory divergence created non-tariff barriers to commerce exchange among EU's member states, undermining another main objective of the Directive—i.e., to ensure free flows of personal data within the internal market.[1035] Further, the lack of harmonization in national data privacy laws created legal uncertainty, generating additional costs and administrative burdens for private firms handling personal data. These problems not only risk

---

[1029] Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INTERNATIONAL DATA PRIVACY LAW 3, 3 (2011) ["*Upcoming Data Protection Reform*"].
[1030] European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Comprehensive Approach on Personal Data Protection in the European Union*, COM(2010) 609 final (November 4, 2010), at 2, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0609&from=EN ["COM(2010) 609"].
[1031] *Id*., at 11.
[1032] *Id*.
[1033] BYGRAVE, *supra* note, at 61. See e.g., EU Data Protection Directive, arts. 5, 9, 13.
[1034] KUNER, *supra*, at 44.
[1035] COM(2010) 609, *supra*, at 10.

creating an unlevel playing field for data operators in the private sector, but also may distort the equivalent level of data protection across Europe.[1036]

(b) The Prominent Role of the DG Just and WP29 and the Institutional Dynamics within the Commission

While these technological, legal, and policy challenges have increased the demand to modernize European data protection framework, there are prominent institutional dynamics at work that make substantial regulatory change politically feasible, shaping the timing, nature, and content of the legal reform.

First, the constitutionalization of data privacy protection in Europe provided both an institutional opening and a normative rationale for the European Commission to develop a comprehensive and coherent framework to reform EU data protection regulation.[1037] As article 8 of the EU Charter became legally binding in Europe in 2009, the EU assumed a positive obligation to implement an effective legal framework to protect data privacy and regulate transfers of personal data.[1038] Further, article 16 of the TFEU created a new legal basis to establish a comprehensive and coherent EU legislation to regulate data processing, including in areas of law enforcement and judicial cooperation in criminal matters.[1039] Meanwhile, these institutional changes also produced a strong normative demand for the EU to strengthen data protection through legislation, in order to give effect to the fundamental rights enshrined in European primary law.

Second, the Lisbon Treaty and EU Charter have strengthened the legal and political position of the DG Just within the Commission with respect to data protection, providing an opportunity structure for its political entrepreneurship.[1040] Notably, the constitutionalization of data privacy protection has framed data protection as a matter of fundamental right, distancing this matter from a purely market-based logic.[1041] As such, it makes legal and political sense for the Commission to delegate the task of data protection reform to the DG Just (focused on protection of fundamental rights and consumers), rather than the DG Market (whose mandate is more market-oriented) or other Directorates-General.[1042] Under the leadership of Viviane Reding, the DG Just seized the "new legal possibilities" created by the Lisbon Treaty to become the lead DG for EU data protection policy, leveraging its agenda-setting power to vigorously push for a reform of existing regulatory framework.[1043] Headed by the experienced and ambitious Commissioner Reding, the DG Just forcefully defended its reform proposals against other Directorate-Generals, and made it much

---

[1036] *Id.* Jones and Kaminski, *supra*, at 105 (noting that such divergence allows "regulatory arbitrage by companies that chose more lax jurisdictions (within the EU)").
[1037] Laurer and Seidl, *supra*, at 9.
[1038] Burri and Schar, *supra*, at 481.
[1039] COM(2010) 609, *supra*, at 4.
[1040] Laurer and Seidl, *supra*, at 9-10.
[1041] *Id.*
[1042] *Id.* See Directorate-General for Justice and Consumers, https://ec.europa.eu/info/departments/justice-and-consumers_en (stating that the DG Just is responsible for EU policy on the protection of fundamental rights, protection of personal data, and protecting and empowering consumers, among others); Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG Market), https://ec.europa.eu/growth/about-us_en (the DG Market's mandate is more market-oriented, focused on the economic areas of European policies).
[1043] Laurer and Seidl, *supra*, at 9.

harder for business interest groups to have their voices heard, despite their fierce lobbying during the policy formulation stage.[1044]

This strong pro-reform position of the DG Just was in stark contrast with that of other Directorates-General. For instance, the Directorate-General for Information Society and Media, which led a review of the EU Data Protection Directive for the Commission in 2007, found against amending the Directive.[1045] In comparison, the Commission's attitude shifted considerably since 2009 when the DG Just took the lead on this matter. After a review of existing EU legal framework followed by a public consultation, the European Commission concluded, in a 2010 Communication, that it was necessary to reform EU data protection regulation to address new regulatory challenges.[1046] Building on the institutional opening created by the Lisbon Treaty, the Commission decided to develop a comprehensive legal framework to modernize EU data protection law, in order to enhance the fundamental right of data protection and improve data transfers within the single market.[1047]

Third, the content of the proposed regulation was substantially influenced by the WP29, providing the legal and regulatory expertise to reform European data privacy regime. Established by the Directive, the WP29 not only consolidated national DPAs' transgovernmental network, but also was mandated with an official role in advising the Commission on any amendments to the Directive.[1048] In 2009, the DG Just provided the secretariat to the WP29, and the Commission consulted the WP29 during the EU's first public consultation on the legal framework for the fundamental right to personal data protection.[1049] In response, the WP29 produced a thorough policy report to the Commission, proposing a comprehensive legal framework with updated rules to address new regulatory challenges.[1050] This gave the WP29 an outsized influence in shaping the final legal solution adopted by the Commission. A textual comparison between the WP29's report

---

[1044] Laurer and Seidl, *supra*, at 9 (noting that "in the words of Ms. Reding herself, lobbying during the policy formulation was 'fierce—absolute fierce' but that 'the legislation was on the table' as Ms. Reding 'wanted to have it'").

[1045] Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council on the Follow-up of the Work Programme for Better Implementation of the Data Protection Directive*, COM(2007) 87 final (March 7, 2007), at 9, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0087:FIN:EN:PDF (concluding that the Directive "*should not be amended*… The Commission will pursue proper implementation of its provisions at national and international level… and will produce an interpretative communication on some provisions"); Jockum Hildén, *The Politics of Datafication: The Influence of Lobbyists on the EU's Data Protection Reform and Its Consequences for the Legitimacy of the General Data Protection Regulation*, PHD Dissertation (on file with the author), November, 2019, https://helda.helsinki.fi/handle/10138/305981 (noting that the Directorate-General for Information Society and Media was in charge of the 2007 review of the Directive). Likewise, the DG Market launched a review of the Directive in 2002, and did not find in favor of reform either. See *id.*; European Commission, *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, May 15, 2003, at 27.

[1046] COM(2010) 609, *supra,* at 3-5. Reding, *supra* (Upcoming Data Protection Reform), at 4.

[1047] COM(2010) 609, *supra,* at 4-5 (stating that "the Commission will give the highest priority to ensuring respect for the fundamental right to data protection throughout the Union and all its policies, while at the same time enhancing the internal market dimension and facilitating the free flow of personal data").

[1048] EU Data Protection Directive, arts. 29, 30(1)(c). See *supra* Section II.C.(D).

[1049] The Future of Privacy, *supra*, at 1-2 (stating that in this consultation, the Commission asked questions on "whether the current legal framework meets (new) challenges and what future action would be needed to address (them)"). See COM(2010) 609, *supra,* at 3 (fn.3).

[1050] See generally The Future of Privacy, *supra.*

and the final text of the GDPR suggested that the former has contained many key elements of the latter.[1051] As observed by commentators, "many of the WP29's demands from 2009 not only made it into the Commission's 2012 proposal but even into the final text of the GDPR."[1052] By partnering up with the DG Just, the WP29 was further empowered in the EU's policy-formulation process leading to the GDPR. As such, the WP29 has gained a privileged position to leverage its expertise to shape the new regulation, transposing its policy preferences into the Commission's legislation.

(c) Geo-political and Geo-economic Considerations

While its primary motivations underlying the proposed GDPR originated from an inward-looking political agenda (i.e., ensuring protection of fundamental rights and enhancing the single market),[1053] the Commission was increasingly aware of the need to use its regulatory capacity to externalize European data protection rules globally.[1054] In a 2009 Communication, the Commission stressed that "the Union must be a driving force behind the development and promotion of international standards for personal data protection," meanwhile stating that EU data privacy law "could serve as a basis" when concluding future bilateral or multilateral agreements.[1055] Building on such an external regulatory agenda, the Commission used this rationale to promote and rally political support for a proposed legislation (i.e., the GDPR) aimed at revising existing legal framework and strengthening data protection.[1056] Calling for developing European data privacy law as "a benchmark for third countries,"[1057] the Commission argued that "[a] high and uniform level of data protection within the EU will be the best way of endorsing and promoting EU data protection standards globally."[1058] As such, the Commission has been increasingly pursuing an external agenda to globalize EU data protection norms as international standards, making the EU a global rule-maker of data privacy. Supplementing its internal agenda (which remains paramount), this outward-looking motivation lends further support for the Commission to push for the GDPR, as it could provide a model of universal data privacy principles based on EU norms and reflecting EU values. Indeed, as publicly stated by the DG Just Věra Jourová in 2017 (the year before the GDPR became effective): "We want to set the global standard…. Privacy is a high priority for us."[1059]

[1051] Laurer and Seidl, *supra*, at 9. For a comparison chart, see *id.*, at 10.

[1052] *Id.*, at 9-10 (noting that "the Commission's proposal bears the hallmarks of the WP29 and not of data-driven businesses"). See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[1053] COM(2010) 609, *supra*, at 2-10, 18.

[1054] BRAFORD, *supra* (BRUSSELS EFFECT), at 18, 21-22. See *id.*, at 16, 19.

[1055] Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council: An Area of Freedom, Security and Justice Serving the Citizen*, COM(2009) 262 final (June 10, 2009), at 9, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:en:PDF.

[1056] COM(2010) 609, *supra*, at 16, 18-19.

[1057] *Id.*, at 16 ("Data processing is globalised and calls for the development of universal principles for the protection of individuals with regard to the processing of personal data… (the) effect and impact (of EU data privacy law), within and outside the Union, have been of the utmost importance. The European Union must therefore remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on relevant EU and other European instruments on data protection").

[1058] *Id.*, at 19.

[1059] Mark Scott and Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (January 31, 2018), https://perma.cc/PKM3-BA3V.

Moreover, in the aftermath of the 2013 Edward Snowden's revelations exposing widespread practices of US Internet platform giants sharing personal data with US national security agencies, the issue-salience of data privacy protection rose to an unprecedented level in Europe. Despite intensive lobbying efforts from U.S. business groups and digital industries to water down the GDPR,[1060] this drastic change in the political dynamics prompted key EU policymakers to distance themselves from business interests, and made it far more difficult for U.S. lobbyists to have their voices heard in Brussels.[1061] Within the Council and Parliament, data privacy advocates were further empowered, and the pro-GDPR coalition grew stronger, as most parliamentary actors and many member states (including Germany and France) joined this camp.[1062] In the context that the U.S. has been increasingly "weaponizing" global telecommunication networks (by turning them into massive surveillance apparatus), [1063] the GDPR provides not only robust institutional safeguards of Europeans' fundamental rights to data protection and privacy, but also an instrumental tool for the EU to reassert its digital sovereignty in international political-economic competition.[1064] Shifting the power balance in favor of the pro-reform camp against business interest groups, such institutional dynamics were instrumental for the Council and Parliament to adopt the GDPR.[1065]

(B) The GDPR

In April 2016, the European Union adopted the GDPR after more than four years' intensive negotiations. This sub-section provides a comprehensive comparison between this legislation and the EU Data Protection Directive, suggesting the legal and policy outcomes created by this lawmaking process. While an in-depth analysis of every change is outside the scope of this work, it hopes to capture essential features of the GDPR's approach to regulating data privacy protection and cross-border data flows, indicating salient trends in this round of legal reform.

(a) A Harder Law with an Extended Reach

Perhaps the biggest change brought about by the GDPR is that it creates a harder law.[1066] Unlike the Directive that required implementation through national laws, the GDPR directly applies to all

[1060] Laurer and Seidl, *supra*, at 11-12 (noting that "the Commission's original proposal was on the brink of being substantially watered down in the spring of 2013", and "these lobbying efforts were initially successful in amending the Commission's proposal in ways that reflect business interests").
[1061] *Id.*, at 12-13, 16 (noting that "[t]he 'salience shock' that followed these revelations fundamentally changed the public debate around data protection and tarnished the reputation of tech companies, which were perceived as 'enablers of state surveillance'").
[1062] *Id.*, at 15. In contrast, the European Commission 2012 proposal for the GDPR only received a "cool reception" from many member states from the outset, and some (such as Germany, Ireland, Sweden, and the UK) strongly opposed it. See id., at 12.
[1063] Henry Farrell & Abraham Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INTERNATIONAL SECURITY 42 (2019).
[1064] Laurer and Seidl, *supra*, at 16. See Anupam Chander & Haochen Sun, Sovereignty 2.0, VANDERBILT J. TRANSN'L L. 2021 (forthcoming), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3422&context=facpub, at 1, 10 (Defining "digital sovereignty" as the "application of traditional state sovereignty over the online domain", meaning a sovereign actor's capacity to regulate and exercise control over the internet).
[1065] Laurer and Seidl, *supra*, at 12-16.
[1066] Jones and Kaminski, *supra*, at 106.

EU member states (including EEA members), in order to achieve greater harmonization among national laws and enforcement policies.[1067] Aligned with the fundamental right nature of data protection, this legislative choice represents a notable departure with the established legislative path of EU consumer law, which typically uses directives (not regulations) to protect individuals. [1068] Meanwhile, the Regulation considerably sharpens its sanctions, creating substantial deterrence to secure compliance of multinational firms. Specifically, it allows national DPAs to impose an administrative fine up to 20 million Euros or 4% of the firm's worldwide total revenue, whichever is higher.[1069]

Compared with the Directive, the GDPR also substantially expands its scope of application. First, the Regulation broadens the extraterritorial reach of the Directive. In addition to covering firms established in the EU (irrespective of where the processing occurs), the Regulation also applies to non-EU firms, where they (a) offer goods or services to EU data subjects (even if no payment is required), or (b) monitor the behavior of data subjects in the EU.[1070] In this way, U.S. digital giants offering online services in a language or currency generally used in an EU member state, or otherwise mentioning EU customers or users in their marketing activities, may be deemed "targeting" EU individuals, and thus could be governed by this legislation.[1071] This extended extraterritoriality evinces the EU's enhanced commitments to safeguard the fundamental right to data protection, even if the underlying data are processed outside Europe.[1072]

Second, the Regulation brings data *processors* into the ambit of EU data protection rules, obliging them to fulfill many responsibilities similar with those of data *controllers*. Unlike the Directive that imposed most duties on data controllers, the GDPR substantially extends obligations to data processors (which process data on behalf of controllers), striking a better balance when assigning responsibilities on digital firms. [1073] For instance, the Regulation creates general duties on processors,[1074] requires them to assist controllers in ensuring secure data processing[1075] and to cooperate with DPAs,[1076] and imposes specific duties for certified processors.[1077] Further, while under the Directive only controllers are liable for non-compliance with data protection rules, the GDPR subjects processors to data subjects' claims for damage, and to regulators' administrative fines, as are controllers.[1078] In addition, under the GDPR, a data processor that jointly determines

[1067] That said, the GDPR also allows for numerous derogations by member states, which may pass implementing laws with potential variations. See e.g., GDPR, arts. 85-91 (mandating member states to develop national laws for the processing of personal data on health, processing in employment context, processing for scientific or historical research or statistical purposes, or processing by churches and religious associations); See Jones and Kaminski, *supra*, at 105-6.
[1068] Schwartz and Peifer, *supra*, at 129.
[1069] GDPR, art. 83.
[1070] GDPR, art. 3.
[1071] GDPR, Recital 23.
[1072] The Future of Privacy, *supra*, at 9.
[1073] Lilian Edwards, *Data Protection: Enter the General Data Protection Regulation*, in LAW, POLICY AND THE INTERNET 6 (Lilian Edward ed., 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3182454. BYGRAVE, *supra*, at 73.
[1074] GDPR, arts. 28 (general duties of processing), 30 (requiring processors to document their processing activities, just like controllers must do).
[1075] GDPR, arts. 32-35.
[1076] GDPR, art. 31.
[1077] GDPR, arts. 42-43.
[1078] GDPR, art. 82

the purposes and means of the processing with a controller may be deemed a "joint controller", and thus should be equally liable for controller obligations.[1079]

As observed by a commentator, the GDPR "moves towards giving the processor an independent existence", making it emerge from the shadows.[1080] In this way, the individual rights and corporate obligations under the GDPR become much more attached to the personal data concerned, irrespective of which entity holds the data. This marks a notable distinction from U.S. data privacy law, which primarily focuses on protecting individuals in direct consumer relationships with companies, leaving a growing sector of processing activities (especially those by third-party data brokers) largely unregulated.[1081] Moving away from the binary division between controllers and processors under the Directive, the GDPR has considerably expanded the obligations of processors. This change may be instrumental for addressing the uncertain legal status of cloud service providers (especially U.S. digital giants) and other novel data brokers, given that cloud computing and targeted advertising make it increasingly hard to distinguish controllers and processors.[1082]

(b) Enhancing Individual Rights to Further Empower Data Subjects

Building on the Directive as a baseline, GDPR further strengthens the substantive and procedural rights of individuals, empowering data subjects to play a more active role in protecting their data.

First, the Regulation reinforces pre-existing individual rights under the Directive. This is the case with the right to access. Building on article 12 of the Directive, the GDPR adds new elements into this right. These include data subjects' capability to obtain information from the controllers on (i) the envisaged or applied storage period, and (ii) the existence of the rights to rectification or erasure, to restrict or object to data processing, and to lodge a complaint with a competent DPA.[1083] Such an enhanced right makes it easier for data subjects to access their personal data, strengthening individuals' ability to verify the accuracy of such data and the lawfulness of the processing.[1084]

Another prominent instance is the right to be forgotten (or the right to erasure). As held by the ECJ in the *Google Spain* case, this right was already encompassed in the Directive's right to access (article 12(b)) and right to object (article 14).[1085] However, it was difficult for data subjects to invoke this right to have unlawfully processed personal data deleted.[1086] Under the GDPR, the right to be forgotten is formally codified as a standalone right in article 17, with extended and clarified normative elements and a stronger bite. Under this provision, this right's scope of application is also broader than in *Google Spain*, as it applies to all data controllers (not just search

[1079] GDPR, art. 26 (defining the concept as "two or more controllers jointly determine the purposes and means of processing"); Recital 79.
[1080] Peter Blume, *Controller and Processor: Is There a Risk of Confusion?*, 3 INT'L DATA PRIVACY L. 140, 144 (2013).
[1081] See Jones and Kaminski, *supra*, at 107.
[1082] Edwards, *supra*, at 6-7 (noting "a strong case … that every party who processes data should simply apply all data protection obligations as far as is practically possible and the doomed attempt to construct a binary division be abandoned").
[1083] GDPR, art 15(1)(d)-(f). Compare with article 12 of the EU Data Protection Directive.
[1084] Reding, *supra* (European Data Protection Framework), at 125.
[1085] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, ¶¶ 97-98 (May 13, 2014).
[1086] Reding, *supra* (European Data Protection Framework), at 125.

engines).[1087] Specifically, individuals are entitled to request a data controller to delete their data without undue delay, if (i) the data are no longer necessary regarding the original purposes for which it was collected or processed, (ii) the data subject withdraws his consent or objects to the processing, or (iii) the processing of data otherwise is unlawful under the Regulation.[1088]

Second, the GDPR has introduced new rights for data subjects. A notable instance is the "right to data portability". This right enables a data subject to obtain from the data controller a copy of his personal data "in a structured, commonly used and machine-readable format", where the data processing is automatic, and based on consent (or necessary for the performance of a contract).[1089] Also, a data subject is entitled to transfer those data from one controller to another without hindrance, as far as technically feasible.[1090] In addition, the Regulation creates new individual rights specific to algorithmic decision-making. These include a right to be notified of the existence of solely automated decision-making (including profiling),[1091] a right to be informed of the significance and envisaged effects of such processing,[1092] a right to obtain an explanation of the decision made by algorithms, a right to contest that decision, to express the data subject's point of view, and to obtain human intervention on the part of the controller for such processing.[1093] Countering the increasingly dominant role of digital platforms, these rights enhance the capacities of data subjects to control their data in the context of automated data processing and algorithmic decision-making.

Third, the Regulation improves the means for individuals to exercise their rights and seek legal redress. Most notably, it creates a class-action like legal remedy for data subjects. Under article 80, data subjects may mandate certain public interest entities to lodge a complaint with a national DPA, challenge a DPA's binding decisions, pursue judicial remedy against a data operator before court, and receive compensation for damage suffered.[1094] This provision enables qualified NGOs, consumer protection associations, and data privacy associations to assist data subjects with invoking their individual rights, alleviating the difficulty in seeking administrative and judicial redress.

(c) Strengthening Corporate Governance by Establishing Collaborative Governance

In addition to enhancing data subjects' rights, the GDPR has also developed a more elaborate system of regulatory compliance obligations for companies to fulfill, regardless of whether the individuals invoke their rights.

First, the Regulation establishes a "privacy by design and by default" obligation, aimed to integrate data privacy protection into information and communication technologies as well as organizational

[1087] Edwards, *supra*, at 41.
[1088] GDPR, art. 17(1)(a)-(d).
[1089] GDPR, art. 20(1).
[1090] GDPR, art. 20(1)-(2).
[1091] GDPR, arts. 13-14.
[1092] GDPR, arts. 13-15.
[1093] GDPR, art. 22(3), Recital 71.
[1094] GDPR, art. 80. See *id*., arts. 77-79, 82.

processes and infrastructure.[1095] Under this requirement, the technologies used to process personal data should be designed and constructed in a way to minimize data processing (including the amount of data, the period of their storage and accessibility, and the extent of processing), pseudonymize personal data as far as possible, and enhance the transparency of the processing activities.[1096] Thus, data controllers should take technological measures (including encryption, pseudonymization, and access control) to ensure that privacy is protected, monitored, and secured by default.[1097]

In terms of organizational measures, this obligation requires many companies to establish internal data protection officer (DPO).[1098] An independent data protection expert reporting to the highest management of the firm, the DPO must be mandated to monitor compliance, provide advice, and act as the contact point to cooperate with the DPAs.[1099] The company shall provide the DPO with access to information and resources necessary for performing its tasks.[1100] By adding an layer of responsibility, the DPO is designed to embed data protection into an organization's internal practice and policy, and may contribute to the development of sector-specific best practices regarding data privacy and data processing.[1101]

Second, the Regulation adds the accountability principle as one of the core principles governing data processing, requiring data controllers to "be responsible for, and be able to demonstrate compliance with" the regime.[1102] This principle replaces the Directive's general notification obligation (requiring controllers to notify their local DPAs before their data processing operations), which has increasingly been seen as needlessly cumbersome and bureaucratic.[1103] Instead, the Regulation establishes important corporate compliance responsibilities for data protection at a systemic level, complementing and safeguarding the realization of individual rights.[1104]

At the core, the accountability principle obliges data controllers to carry out necessary internal mechanisms and policies to ensure that substantive data protection principles and obligations are complied with when processing personal data, and to demonstrate their compliance to external stakeholders (including DPAs, third party experts, and the public).[1105] Specifically, the GDPR

[1095] GDPR, art. 25. This principle is not completely new, as the Directive already required data controllers to "implement appropriate technical and organizational measures" to protect personal data. See EU Data Protection Directive, art. 17; Recital 46. But the GDPR reinforces this notion, and develops it into an independent substantive obligation.
[1096] GDPR, art. 25 (including a specific obligation to prevent personal data from being made accessible to an indefinite number of natural persons by default); Recital 78.
[1097] GDPR, Recital 78. The Future of Privacy, *supra*, at 13-14.
[1098] GDPR, art. 37. A data controller or processor shall designate a DPO, where their "core activities… consist of processing operations which… require regular and systematic monitoring of data subjects on a large scale," or include large-scale processing of sensitive personal data. *Id.*, art. 37(1)(b)-(c).
[1099] GDPR, arts. 37-39.
[1100] GDPR, art. 38.
[1101] See Reding, *supra* (European Data Protection Framework), at 127.
[1102] GDPR, art. 5(2).
[1103] Edwards, *supra*, at 21; COM(2016) 609, *supra*, at 12. See EU Data Protection Directive, art. 18. Relatedly, the GDPR introduces a general mandatory notification obligation in case of personal data breaches, enabling DPAs to be more selective and concentrated in their oversight capacity: data controllers must notify DPAs of all personal data breaches, and notify data subjects of high-risk breaches of their personal data. See GDPR, arts. 33-34.
[1104] Jones and Kaminski, *supra*, at 118.
[1105] The Future of Privacy, *supra*, at 20.

requires a data controller to (1) maintain records of its data processing activities,[1106] (2) carry out data protection audits, when so requested by a DPA,[1107] (3) conduct data protection impact assessments prior to initiating potentially high-risk data processing (including large-scale processing of sensitive personal data and systemic monitoring of public places),[1108] and consult with DPAs for particularly risky processing (which can require measures to mitigate the risks), and provide DPAs with requested information (including the impact assessments),[1109] (4) notify DPAs of all breaches of personal data, and notify data subjects of high-risk breaches of their personal data,[1110] among others.

Collectively, the requirements of accountability and privacy by design and by default exemplify the Regulation's approach to corporate governance, bearing the hallmark of "collaborative governance" as a regulatory model.[1111] By outsourcing many governance decisions and enforcement tools to private firms, the GDPR explicitly or implicitly entrusts such companies with determining the substance of their own duties and self-monitoring, evincing the regulatory model of "co-governance" or "public-private partnerships".[1112] But this approach is substantially different from the U.S. model of business "self-regulation", as the government still has an important (if not central) role to play.[1113] Under the GDPR, the systemic corporate governance system not only features extensive top-down rules and guidance aimed at ensuring high-standard data protection, but also is keenly overseen by robust enforcement and oversight mechanisms (i.e., national DPAs with heavy sanctioning powers) and an active human rights court (i.e., the ECJ as the ultimate guardian of fundamental rights).[1114] In particular, as data protection is an European fundamental right that applies to governments and private firms (as is the right to privacy), the GDPR is anchored into the EU's human rights backstop, making the collaborative governance system drastically different from a hands-off, self-regulatory regime.[1115]

(d) Improving Regulation over Cross-Border Flows of Personal Data

Regarding international transfers of personal data, the GDPR adopts the regulatory framework of the Directive, but modifies and improves existing rules and mechanisms on numerous fronts.

[1106] GDPR, art. 30.
[1107] GDPR, art. 58(1)(b).
[1108] GDPR, art. 35; see id, art. 9(1).
[1109] GDPR, art. 36.
[1110] GDPR, arts. 33-34. In lieu of the Directive's general notification requirement of all automatic processing of personal data, the GDPR introduces a general mandatory notification obligation in case of personal data breaches, enabling DPAs to be more selective and concentrated in their oversight capacity. This provision seems to originate from the California's statute and US data privacy law. See Schwartz, *supra* (The EU Way), at 808-9.
[1111] Jones and Kaminski, *supra*, at 118.
[1112] *Id.*, at 119. In many places, the language of the GDPR is formulated in "broad, almost aspirational terms", yet "that vagueness is at least partially intentional… because it tasks companies with figuring out how to best implement its aspirations." And on data protection, "European regulators are often more interested in cooperation and good faith efforts than in perfect compliance." *Id.*, at 110-11. See Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIVACY L. 125, 127 (2021).
[1113] Kaminski and Malgieri, *supra*, at 127. See Reidenberg, *supra* (*Resolving Conflicting*), at1331.
[1114] Jones and Kaminski, *supra*, at 119.
[1115] *Id.*, at 111, 119 (noting that "even if EU regulators might act cooperatively towards companies, there is no guarantee that European courts will do the same. For every vague balancing test conducted by a company under the GDPR, there is the possibility that a court will find that balancing to be inadequate as a matter of fundamental rights").

(1) The Adequacy Process

Following a qualified prohibition approach to cross-border personal data flows, the Regulation further harmonizes the adequacy assessments, introduces "partial" adequacy decisions, and reinforces the Commission's powers and duties to monitor and review its adequacy decisions.

First, the GDPR centralizes the Commission's authority to issue an adequacy decision, and clarifies the criteria for reaching such a finding, aimed at harmonizing the adequacy assessments in Europe. Under the Directive, whether a third country ensures an adequate level of protection may be determined by member states and the Commission.[1116] However, the Directive did not specify in sufficient detail the exact factors for reaching an adequacy finding.[1117] This legal uncertainty led to considerable divergences in member states' national legal approaches to assessing the level of protection in third countries.[1118] It also created the risk that a third country's level of data privacy protection is evaluated differently from one member state to another, undermining the consistency of the adequacy assessments.[1119]

In response, the GDPR shifts the decision-making authority to the exclusive ambit of the Commission, and thus prevents the adequacy assessments from varying among EU member states.[1120] Further, the Regulation enunciates a more precise list of factors to determine the level of data protection of a third country. Such criteria include the substantive data privacy protections applicable to personal data, effective independent oversight authorities and legal redress mechanisms, and the third country's international commitments or legally binding assurances to protect personal data.[1121] Though a point-to-point replication of EU data protection law is unnecessary, that third country's legal system as a whole should ensure an "essentially equivalent" level of protection compared with EU law.[1122] These aspects help to strengthen the legal certainty, coherence, and uniformity of the EU's adequacy determinations.

But in addition to these legal considerations, the Commission's adequacy process has long contained political and strategic elements. In a 2017 Communication, the Commission articulated several core criteria for selecting third countries for entering "a dialogue" on adequacy decisions (rather than for assessing the "adequacy" *per se*). These include (1) "the extent of the EU's (actual or potential) commercial relations with" that third country, including the presence of "a free trade agreement or ongoing negotiations"; (2) "the extent of personal data flows from the EU", (3) "the pioneering role" that third country plays in privacy and data protection, providing "a model for other countries in its region", and (4) "the overall political relationship with" that country,

[1116] Under the Directive, member states must incorporate the adequacy process into their domestic laws; meanwhile, the Commission may find a third country's data privacy protection (in)adequate. See EU Data Protection Directive, art. 25(1), (4), (6).
[1117] COM(2010) 609, *supra*, at 15. See Id., at 25(2).
[1118] COM(2010) 609, *supra*, at 15 ("In some Member States adequacy is assessed in the first instance by the data controller which itself transfers personal data to a third country, sometimes under the ex-post supervision of the data protection supervisory authority"); KUNER, *supra*, at 44.
[1119] COM(2010) 609, *supra*, at 15.
[1120] GDPR, art. 45(1).
[1121] GDPR, art. 45(2); Recital 104-105.
[1122] GDPR, Recital 104. See *Schrems I*, paras. 73, 74, 96.

particularly regarding "the promotion of common values and shared objectives at international level".[1123] When choosing third countries to start adequacy discussions, the EU thus looks to such non-legal criteria to pursue instrumental goals, including strengthening the influence of EU data protection law, increasing regulatory convergence of foreign data protection laws and practices, and expanding Europe's external commercial relations with those markets.[1124] With these strategic considerations in mind, the EU may prioritize its adequacy discussions and negotiations with certain key trading partners over others.[1125]

Second, building on the practice under the Directive, the Regulation explicitly authorizes the Commission to issue a "partial" adequacy decision, in addition to a country-wide finding.[1126] Under the GDPR, the Commission may decide that a particular territory of a third country or one or more sectors of its economy provides an adequate level of protection.[1127] For example, the EU's findings on the U.S. (limited to the EU-US Safe Harbor and Privacy Shield frameworks) and Canada are "partial" adequacy decisions.[1128] Moving away from an all-or-nothing approach, this revision brings more diversity to the EU's adequacy findings, enhancing the interoperability between different data privacy regimes.

Third, the Regulation mandates the Commission to closely monitor existing adequacy findings through periodic review mechanisms, transforming such decisions from a *fait accompli* into "living" instruments that require constant stewardship and adaptations. Prior to the GDPR, this obligation was firstly imposed by the ECJ in *Schrems I*, a case against the Safe Harbor (a tailor-made instrument to transfer personal data from the EU to the U.S.). In that case, the Court required the Commission to check periodically whether its adequacy decision was "still factually and legally justified", when evidence raised a doubt on the adequacy of the level of protection ensured by a third country.[1129] Building on that ruling, the Regulation extends this obligation to all of the Commission's adequacy decisions.

Under the GDPR, the Commission must conduct periodic reviews to monitor its adequacy decisions, adapting them to any subsequent developments potentially affecting the level of protection concerned.[1130] This obligation also applies to existing adequacy decisions adopted by the Commission under the Directive.[1131] When finding that a third country's protection no longer meets the required standard, the Commission is empowered to repeal, amend, or suspend the adequacy decision, and may launch consultation with that country to remedy the issues

---

[1123] European Commission, *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7 final (January 10, 2017), at 8, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN ["COM(2017) 7"].
[1124] *Id.* Chander and Schwartz, *supra*, at 32 (arguing that the EU acknowledged and sought to leverage the "instrumental nature" of its process for choosing third countries to pursue adequacy discussions).
[1125] COM(2017) 7, *supra*, at 8, 10 (noting that the EU's priorities in this area include Japan, Korea, Latin America countries (particularly Mercosur member states), and the European neighborhood).
[1126] *Id.*, at 4.
[1127] GDPR, art. 45(1); Recital 103.
[1128] COM(2017) 7, *supra*, at 7 (explaining that the EU's adequacy finding on the US only applies to US firms opting in the Privacy Shield, and its adequacy decision on Canada "applies only to private entities falling under the scope of the Canadian Personal Information Protection and Electronic Document Act").
[1129] *Schrems I*, para. 76.
[1130] GDPR, art. 45(4); Recital 106.
[1131] GDPR, art. 45(4); Recital 106.

identified.[1132] In this way, the Regulation expands and sharpens the scrutiny of the Commission's adequacy assessments, and strengthens the obligations of third countries to continuously ensure a level of protection equivalent to EU law.

(2) Alternative Transfer Mechanisms

In addition to modifying the adequacy process, the Regulation also reinforces, streamlines, and diversifies alternative transfer mechanisms (termed as "appropriate safeguards") to facilitate transborder personal data flows, adding flexibility to accommodate the needs of numerous transfer situations. Though ensuring high-standard protection of personal data is non-negotiable for the EU, the GDPR provides a broader and more varied transfer toolkit to facilitate personal data flows in different circumstances, meanwhile seeking to maintain a sufficient level of protection.[1133]

First, the GDPR solidifies and extends the use of existing accountability mechanisms (i.e., SCCs and BCRs) under the Directive, and make them more adapted to specific business needs.[1134] Unlike the Directive, the Regulation explicitly recognizes BCRs as a valid alternative mechanism to export personal data.[1135] Aligned with the new obligations assumed by data processors, SCCs and BCRs under the Regulation can apply to data transfers between processors.[1136] In particular, this may facilitate transfers of personal data by cloud service providers.[1137] Also, while the Directive limited the use of BCRs to corporate entities of the same corporate group, the GDPR allows them to apply to transfers between different corporate groups engaged in joint economic activities.[1138] For instance, different flight carriers belonging to the same airline alliance now can use BCRs to transfer personal data with each other.[1139] These new possibilities help to develop sector-specific SCCs and BCRs tailored to the needs of specific industries, business models, and operators.[1140]

In addition, the Regulation introduces new alternative mechanisms to transfer personal data to third countries. These include approved codes of conduct or accredited third-party certifications (such as privacy seals or marks), designed to ensure and demonstrate the exporters' compliance with the GDPR's requirements.[1141] While their implementation remains to be seen, the Commission hoped that these mechanisms could provide more customized transfer tools catering to a specific industry, sector, or a particular type of data processing, meanwhile constituting new components of the Regulation's compliance infrastructure.[1142]

[1132] GDPR, art. 45(5)-(6); Recital 107.
[1133] COM(2017) 7, *supra*, at 6.
[1134] *Id.*, at 4, 11.
[1135] See GDPR, art. 47.
[1136] GDPR, Recital 168; COM(2017) 7, *supra*, at 10.
[1137] European Union, *Digital Single Market—Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers*, January 10, 2017, https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_17_15 (Communication QA).
[1138] GDPR, art. 47; Recital 110; COM(2017) 7, *supra*, at 10.
[1139] Communication QA, *supra*.
[1140] *Id.*
[1141] GDPR, art. 46(2)(e)-(f). It bears noting that such newly added "appropriate safeguards" also include "a legally binding and enforceable instrument between public authorities or bodies" as well as approved administrative arrangements containing "enforceable and effective data subject rights" between these actors. See GDPR, art. 46(2)(a), 46(3)(b).
[1142] COM(2017) 7, *supra*, at 5, 10-11.

Second, the Regulation seeks to harmonize the regulatory framework governing international transfers of personal data, and to streamline the administrative process for the approval and usage of SCCs and BCRs. Notably, the GDPR establishes a "one-stop-shop" mechanism: where the processing of personal data involves multiple member states, the DPA of the place where a controller or processor has its main (or single) establishment is competent to act as the lead supervisory authority to regulate its cross-border processing activities throughout Europe.[1143] This new mechanism not only reduces red tape for data operators, but may improve the consistency and legal certainty in applying EU law.[1144] Further, for companies using BCRs to transfer data, the Regulation allows them to apply to a lead DPA for BCR authorization,[1145] instead of applying for approval from DPAs of all member states concerned by a BCR (as required by the Directive).[1146] In addition, as the GDPR abolishes companies' general notification duty prior to data processing, data controllers and processors no longer need to notify DPAs and obtain their specific authorizations for data transfers under SCCs and BCRs.[1147] As such, the simplified process for the accountability mechanisms undercuts the administrative burdens for companies, avoids divergent national regulatory requirements, and facilitates cross-border transfers of personal data.

(e) Reinforcing Enforcement Mechanisms

Finally, the GDPR further enhances the independence, competence, and powers of DPAs, as well as their transnational cooperation. While the Directive made the creation of national DPAs mandatory, the degree of their independence, resources, and powers still varied widely across different member states, and their cooperation at the EU level did not always result in consistent enforcement.[1148] In response, the Regulation specifies in more detail the conditions for the establishment and operation of DPAs to ensure their independence,[1149] harmonizes their competences and duties,[1150] and further reinforces their regulatory powers.[1151] In particular, DPAs are vested with stronger powers to launch investigations,[1152] impose sanctions (including a ban or restrictions on data flows, injunctions, and administrative fines),[1153] render binding decisions

[1143] GDPR, art. 56; Recital 124.
[1144] Reding, *supra* (EU Data Protection Framework), at 128.
[1145] GDPR, art. 56.
[1146] The Future of Privacy, *supra*, at 11. See Wanne Pemmelaar et al, *BCRs under the GDPR: Practical Considerations*, ALLEN OVERY MEDIA (March 2017), at 7-8, https://www.allenovery.com/-/media/wordpressimport/aodigitalhub/bcrs-under-the-gdpr-article.pdf (Under the Directive, the process for applying BCR approval takes about nine months. "A company applies to a lead DPA and two co-lead DPA for authorisation… once approved, the company can apply to national DPAs for authorisations or permits for data transfers under the BCRs").
[1147] GDPR, art. 46(2); COM(2017) 7, *supra*, at 5.
[1148] Reding, *supra* (European Data Protection Framework), at 127 (noting that "[i]n some cases, (national DPAs) are unable to perform their enforcement tasks in a satisfactory way"); The Future of Privacy, *supra*, at 21-22 (stating that the divergent position of DPAs in EU member states are due to the lack of precision of the Directive provisions regarding their creation and operation, as well as the insufficient implementation of the Directive in some countries).
[1149] GDPR, arts. 52-53.
[1150] GDPR, arts. 55-57.
[1151] GDPR, art. 58.
[1152] GDPR, art. 58(1).
[1153] GDPR, art. 58(2).

(including authorizations),[1154] and conduct advisory activities (including counseling national legislative process).[1155]

In addition, the GDPR also creates separate provisions to improve DPAs' transnational cooperation, imposing obligations for a DPA to conduct investigations and inspections upon the request of another DPA, to provide mutual assistance, and to conduct joint operations.[1156] These efforts solidify and reinforce national DPAs' domestic status, power resources, and horizontal networks, enabling them to play a stronger supervision role in safeguarding Europeans' data protection.

IV. TRANSATLANTIC COMMERCIAL DATA TRANSFERS AND ECJ-LED FORUM SHIFTING TO (RE)SHAPE THE "ADEQUACY" STANDARD

This Part proceeds to analyze another law-making process to establish rules governing transatlantic personal data transfers for commercial purposes, focused on the role of ECJ-led forum-shifting in (re)shaping the Commission's "adequacy" requirements. Section A discusses the negotiations and collapse of the Safe Harbor agreement. Section B turns to the establishment and demise of a successor agreement, the Privacy Shield. Section C summarizes the implications of EU data privacy regime for transnational commercial data transfers.

A. The Safe Harbor Agreement and the ECJ Decision of Schrems I

Each adopting drastically different data privacy regimes,[1157] the U.S. and the EU have long maintained substantial regulatory divergence over how personal data should be transferred across national borders. While the U.S. favors unrestricted transnational data flows by default,[1158] EU data protection regulation adopts a qualified prohibition approach, banning data transfers to third countries without "adequate" data protection. By threatening to block transatlantic data flows, the EU's data transfer regulation caused the U.S. to negotiate an international institution with the Commission as a way out of a potential "trade war", resulting in the Safe Harbor agreement.

While some EU privacy activists were dissatisfied with this arrangement, they can neither access the international negotiating forum nor directly influence the Commission's determinations, and thus were unable to push through major institutional change. However, after the rights to data protection and privacy were enshrined in EU primary law as fundamental rights, European courts started to share their normative concerns over the legality of transatlantic data transfers under the EU Charter, opening an alternative institutional pathway for the EU data privacy community to challenge the Commission's adequacy decisions. After the Snowden revelations exposed the links between commercial data transfers and intelligence data sharing, the ECJ leveraged this clash of

---

[1154] GDPR, art. 58(3).

[1155] GDPR, art. 58(3). Under the Directive, DPAs can only counsel the drafting of "*administrative measures or regulations*" regarding individual's personal data protection. The GDPR expands DPAs' advisory authority, enabling them to issue opinions "on *any issue* related to the protection of personal data" to national parliament or governmental bodies (emphasis added). See EU Data Protection Directive, art. 28(2).

[1156] GDPR, arts. 60-62.

[1157] See Schwartz and Peifer, *supra*, at 121-56.

[1158] See Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECO. L. 245, 254-56 (2018).

rules to assert its dominance in scrutinizing the Commission's adequacy findings, requiring EU citizens' data to be adequately protected from pervasive U.S. surveillance practices.

(A) The Safe Harbor

With the implementation of the EU Data Protection Directive, the EU threatened to ban transfers of personal data to any third countries with inadequate level of data protection.[1159] The U.S. was not one of the whitelist countries with adequate data protection.[1160] While U.S. companies are entitled to use SCCs and BRCs to export personal data from the EU, these contractual arrangements impose relatively stringent standards, are inflexible and cumbersome to use, and create high compliance costs.[1161] Thus, an adequacy finding by the Commission provides the "most trade-friendly solution" to international personal data transfers, while ensuring high-level data protection standards.[1162] Though the large market of the U.S. buffered many domestic firms from the extraterritorial effects of the Directive, U.S. multinationals came under considerable pressure of impeded market access, as well as heightened operational and compliance costs.[1163]

Under this "adequacy" approach to international data transfers, the U.S. was pressured to negotiate the Safe Harbor agreement with the EU in 2000, which is a *sui generis* institutional solution to transfer Europeans' personal data for U.S. companies.[1164] Without requiring major institutional reforms from the U.S., this arrangement was designed to work as an institutional interface between two drastically different data privacy regimes,[1165] in order to facilitate and enable unrestricted transatlantic personal data flows on the Commission's acceptable terms to protect EU citizens' data.

Rather than an international trade agreement, this instrument establishes a voluntary opt-in system for the private sector, backed up by structured oversight mechanisms. Under the Safe Harbor, participating U.S. companies self-certify their adherence to a set of substantive EU data privacy principles ("Safe Harbor principles") to demonstrate their compliance with the Directive.[1166] Compliance with these principles is overseen by the regulatory authority of the Free Trade Commission (FTC) or U.S. third-party private organizations.[1167] Meanwhile, European national

[1159] See *supra* section II.B.(C); EU Data Protection Directive, art. 25(4) (where the Commission found a third country did not ensure an adequate level of personal data protection, member states are obliged to take the necessary measures to prohibit any transfer of personal data to that country).
[1160] Schwartz, *supra* (The EU Way), at 793.
[1161] *Id.*, at 794; See *supra* section II.B.(C).
[1162] Chander and Schwartz, *supra*, at 19.
[1163] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 103.
[1164] Commission Decision 2000/520/EC, of 26 July 2000, Pursuant to Directive 95/46/EC, 2000 O.J. (L215) 7 ["Safe Harbor Decision"]; MARTIN A. WEISS & KRISTIN ARCHICK, U.S.-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 1 (2016), Congressional Research Services: R44257.
[1165] FARRELL & NEWMAN, *supra*, at 157.
[1166] Safe Harbor Decision, *supra*, at 8, 10-12 (These principles include notice, choice, onward transfer, security, data integrity, access, and enforcement); HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 132 (2019).
[1167] Safe Harbor Decision, *supra*, at 12. U.S. companies may use private companies, such as BBBOnline or TRUSTe, to handle consumer complaints and resolve privacy disputes. This private third-party dispute settlement mechanism epitomizes a self-regulatory model to oversee compliance, supported and backed up by the enforcement of the FTC, see *id.*, at 40; Schwartz, *supra* (The EU Way), at 797.

DPAs could block data exports, where a U.S. oversight body finds a U.S. firm violative of these principles, or alternatively, may suspend data flows unilaterally, but on relatively restrictive conditions.[1168] The European Commission found self-certified U.S. firms as meeting the "adequacy" standard under the Directive when exporting EU personal data to the U.S.[1169] This hybrid arrangement represents a workable compromise to both sides out of multiple years of negotiations.

On the U.S. side, the government wanted to safeguard and promote its preferred self-regulatory privacy regime.[1170] Domestically, the US has long practiced a sectoral approach to data privacy protection. With legislative rules covering only certain sensitive sectors, the primary source of data privacy protection is industry self-regulation.[1171] And there was no specialized governmental regulator providing independent oversight for data privacy concerns.[1172] Unlike many of the EU's trading partners that followed European data protection approach, the U.S. government desired to protect its own regulatory approach to data privacy, rather than enacting a comprehensive data privacy regime modelled on EU law.[1173] Moreover, concerned that top-down governmental regulation may stifle the development of e-commerce in its infancy, the U.S. hoped to shield American e-commerce firms from stringent foreign regulation, and to encourage the global spread of a laissez-faire approach favoring business self-regulation.[1174] Indeed, in *The Framework for Global Electronic Commerce*, the Clinton Administration voiced its strong support for private sector initiatives to implement a self-regulatory privacy regime, vigorously promoting this governance model to regulate international electronic commerce.[1175] By creating a voluntary self-regulatory model (including a self-certification programme and a self-regulatory oversight mechanism) to enable personal data transfers to the U.S., the Safe Harbor agreement well served these prominent interests.[1176]

For the EU side, negotiators likewise wanted to preserve existing EU institutional approach to data protection,[1177] while facilitating external trade flows with the U.S. (being the EU's most important trade partner).[1178] In this regard, the Safe Harbor not only provided a way out of a transatlantic trade war, but also applied EU data privacy principles to protect Europeans' data.[1179] Moreover,

---

[1168] Safe Harbor Decision, *supra*, at 9, art. 3(1). The European Commission may also reverse, suspend the Safe Harbor decision or limit its scope, where it finds the U.S. oversight bodies are not effectively fulfilling their role. See id., art. 3(4).
[1169] Safe Harbor Decision, *supra*, at 8, art. 1(1).
[1170] FARRELL & NEWMAN, *supra*, at 130.
[1171] Reidenberg, *supra*, at 1331.
[1172] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 30.
[1173] FARRELL & NEWMAN, *supra*, at 130.
[1174] *Id.*, at 130-31 (quoting Ira Magaziner: "The U.S. government believes that… in general… governments should stay away from regulating… the Internet…. [D]evelopments should be led by the private sector, and privately established codes of conduct should govern, not government regulations").
[1175] THE WHITE HOUSE, A FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE 18 (1997).
[1176] Henry Farrell, *Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement,* 57 INT'L ORG. 277, 295 (2003) (noting that the success of the safe harbor depends on the U.S. convincing EU representatives to adopt self-regulatory measures).
[1177] FARRELL & NEWMAN, *supra*, at 131-32 (quoting Spiros Simitis, an influential commission adviser: "Americans still have the illusion that they can change the directive, but they can't …. This is not bananas we are talking about…. This is about what we consider a fundamental claim to privacy, and therefore there is a limit to compromise").
[1178] Schwartz, *supra* (The EU Way), at 798-99.
[1179] *Id.*

the Commission hoped that American firms opting into the Safe Harbor could change their corporate practices and internalize European privacy principles, generating endogenous pressures to transform the U.S. privacy regime along the EU model.[1180]

In hindsight, the U.S. view of the Safe Harbor turned out to be more accurate.[1181] By 2015, 4,500 U.S. firms joined the Safe Harbor.[1182] As the transatlantic digital market grew exponentially, U.S. firms profited substantially from the provision of digital products and services, with leading Internet platforms gaining considerable EU market shares.[1183] Meanwhile, the FTC's enforcement actions under the Safe Harbor (which did not start until 2009) was meager in practice, and had never translated into a comprehensive U.S. federal law governing data privacy.[1184] Rather, controversy on whether the Safe Harbor ensured the adequacy standard of data protection long prevailed. In this regard, critiques argued that this arrangement considerably weakened EU data protection rules, particularly because it maintained wide exceptions unseen in EU law and watered down the redress mechanisms for data privacy breaches.[1185]

Despite these concerns, the European Commission, however, declined to suspend the Safe Harbor, but continued to support this agreement during the 2000s by emphasizing its economic rationale.[1186] After the 2013 Snowden revelations exposing that commercial data flows under this instrument had been extensively used for intelligence surveillance by the National Security Agency (NSA), the Commission entered into negotiations with the U.S., pressing for revisions to the Safe Harbor.[1187] However, with strong resistance from the U.S. intelligence authorities, the EU negotiators made little meaningful progress in obtaining explicit U.S. commitments to remedy the national security aspects of the Safe Harbor.[1188]

(B) The ECJ's Decision of *Schrems I*

After data protection and privacy were constitutionalized in EU primary law, European privacy activists found a new legal ground to challenge the Safe Harbor agreement, taking on U.S. platform giants whose data processing practices were widely perceived as in tension with EU data protection rules. In that regard, the most successful initiative was made by Maximillian Schrems, a young Austrian privacy advocate and attorney, who saw U.S. Internet companies as undermining EU data

---

[1180] FARRELL & NEWMAN, *supra*, at 133-34.
[1181] *Id*., at 134.
[1182] Schwartz, *supra* (The EU Way), at 799.
[1183] FARRELL & NEWMAN, *supra*, at 135.
[1184] *Id*., at 134, 136. WEISS & ARCHICK, *supra*, at 9 (noting that "the FTC brough action against only ten companies during the first 13 years of the agreement's existence").
[1185] FARRELL & NEWMAN, *supra*, at 135; Schwartz, *supra* (The EU Way), at 799-800.
[1186] FARRELL & NEWMAN, *supra*, at 135-36. European Commission, *Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final (November 27, 2013), at 6-7, https://eur-lex.europa.eu/resource.html?uri=cellar:4d874331-784a-11e3-b889-01aa75ed71a1.0001.01/DOC_1&format=PDF ("The Safe Harbor scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic…. [I]ts revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened").
[1187] WEISS & ARCHICK, *supra*, at 1.
[1188] FARRELL & NEWMAN, *supra*, at 144.

protection law and threatening Europeans' fundamental rights.[1189] To protect EU rules, Schrems leveraged the information provided by Snowden revelations to link commercial data (processed by American digital firms) with U.S. surveillance practices, and thus gained access to the legal and regulatory institutions previously closed off.[1190]

Initially, Schrems made a complaint to Ireland's data privacy commissioner, calling for an investigation on whether Facebook had met its obligations for data transfers under the Safe Harbor arrangement, as read in light of the Snowden revelations.[1191] When this request was declined, Schrems filed a legal action before the Irish High Court, arguing that the Irish DPA was obliged to investigate whether Facebook was exposing Europeans to a data breach by using the Safe Harbor to transfer their data to the U.S. where the government can readily access such data through intelligence surveillance.[1192] As the Irish DPA contended that its duty of action was preempted by the European Commission's adequacy determination of the Safe Harbor under the Directive, Schrems not only challenged the validity of that data transfer agreement under the EU Charter, but also questioned the Commission's competence to make adequacy findings that may compromise EU data protection law.[1193] Sharing Schrems' normative concerns, the Irish High Court referred the following issue to the ECJ: whether the Irish DPA was bound by the Commission's adequacy determination that the Safe Harbor ensured an adequate level of protection for EU citizens' data, or should open an investigation as Shrems requested.[1194]

This legal battle led to a landmark judgment of the ECJ. In October 2015, the Court stepped in to render a decision in *Schrems v. Data Protection Commissioner* ("*Schrems I*"), invalidating the Safe Harbor agreement.[1195]

In this judgment, the Court firstly found that the Commission's decision on the Safe Harbor does not eliminate or reduce national DPAs' powers conferred by article 8(3) of the EU Charter and article 28 of the Directive to oversee transfers of personal data to a third country.[1196] As held by the ECJ, when hearing a claim lodged by a data subject, national DPAs "must be able to examine, with complete independence, whether the transfer of that data complies with" the Directive, despite the Commission's adequacy decision.[1197] Notably, the right to lodge a complaint with a DPA is guaranteed by the EU Charter, which, as EU primary law, prevails over all the acts of EU

[1189] *Id.*, at 146.
[1190] *Id*.
[1191] *Id*., at 147. Schrems' selection of the forum was strategic: Ireland's favourable tax treatment, highly flexible application of privacy rules, and relatively lax enforcement of data protection made it a most welcome EU jurisdiction to host U.S. digital giants' European operations, which usually were based in that country. Id., at 146.
[1192] *Id*., at 147.
[1193] *Id*.
[1194] *Schrems I*, para. 36. Justice Hogan held that given that the personal data exported by firms (such as Facebook Ireland) to its parent company in the U.S. were capable of being accessed by the NSA in mass surveillance programmes (as suggested by the Snowden revelations), the European Union's data protection rights under the EU Charter of Fundamental Rights were seriously undermined, and it was not clear how the Safe Harbor Agreement can satisfy its provision protecting personal data. See id., at 148.
[1195] *Schrems I*, para. 201.
[1196] *Id*., paras. 53, 57, 63.
[1197] *Id*., para. 57.

institutions when in conflict (including an adequacy decision on the Safe Harbor).[1198] Yet, only the Court has the exclusive jurisdiction to declare this adequacy finding as invalid.[1199]

Moreover, the Court ruled that the Safe Harbor agreement failed to satisfy the requirements of the Directive, as construed in light of the EU Charter, even without examining the content of the Safe Harbor principles.[1200] First, the Court found that the Safe Harbor principles only applied to self-certified U.S. firms in the private sector, but U.S. public authorities were not required to adhere to them.[1201] Relatedly, the Safe Harbor failed to provide effective regulatory institutions to oversee adherence of these principles against U.S. governmental actors, as required by the Directive.[1202] In this regard, the FTC, with its powers limited to commercial disputes, lacked jurisdiction over U.S. public authorities engaging in intelligence surveillance.[1203] Neither were the private dispute resolution mechanisms under the Safe Harbor applicable to measures adopted by the U.S. government.[1204]

Second, the ECJ held that the U.S.'s "'national security, public interest, or law enforcement requirements' have primary over the safe harbour principles," such that self-certified U.S. firms receiving EU data "are bound to disregard those principles without limitation" when these two sets of norms were in conflict and incompatible.[1205] Despite the protections provided by the Safe Harbor principles, when U.S. national security law imposed a conflicting duty, U.S. entities (whether in the Safe Harbor or not) would be obliged to provide EU citizens' data to U.S. governmental actors, even if doing so will interfere with Europeans' fundamental rights under the EU Charter.[1206] Moreover, the Court found that the Safe Harbor, by virtue of its broad derogations, permits U.S. "public authorities to have access on a generalised basis to the content of electronic communications", undermining "the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."[1207]

Third, the Court faulted the Safe Harbor for unduly restricting the enforcement powers of EU national DPAs to block data flows, as guaranteed in the Directive and the EU Charter to ensure effective data protection. As found by the Court, the Safe Harbor stipulated more restrictive conditions for DPAs to suspend data flows to the U.S., establishing a higher threshold for their regulatory intervention than provided under the Directive.[1208] In adopting an adequacy decision for the Safe Harbor, the Commission has exceeded its competence to restrict the powers of national

[1198] *Id*., paras. 58-60. See EU Charter, art. 8(1)(3).
[1199] *Schrems I*, paras. 61.
[1200] *Id*., para. 98.
[1201] *Id*., para. 82.
[1202] *Id*., paras. 88-89.
[1203] *Id*., para. 89
[1204] *Id*.
[1205] *Id*., para. 86.
[1206] *Id*., para. 85 ("…. where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law").
[1207] *Id*., paras. 87, 94.
[1208] *Id*., para. 101. Under the Safe Harbor, EU national DPAs can block data flows only upon a finding by a U.S. regulatory agency or a self-regulatory organization that the U.S. firm is breaching the principles, or may unilaterally block data transfers upon restrictive conditions. See Safe Harbor Decision, *supra*, art. 3(1). Compare with art. 28 of the EU Data Protection Directive.

DPAs as such.[1209] Thus, the Safe Harbor decision, the Court considered, must be regarded as denying the powers of national DPAs to safeguard EU citizens' fundamental rights, and hence is invalid.[1210]

This ruling substantially changed the legal landscape on transatlantic data privacy rulemaking. By grounding the Commission's "adequacy" standard in EU constitutional law, the Court shifted the ultimate decision-making authority to decide the "adequacy" standard from the Commission to itself. In other words, through forum-shifting, the ECJ has become the final arbiter of the Commission's adequacy decisions, establishing the legal and regulatory requirements for transnational data transfers.

First, this judgment constitutionalized the EU's adequacy standard and other aspects of EU data protection law,[1211] and empowered the ECJ, national courts, and national DPAs to scrutinize the EU's adequacy findings for third countries.[1212] Previously, the Commission, with a privileged access to international negotiation channels during the adequacy negotiations, long enjoyed dominance in defining the transatlantic privacy agenda, while other more privacy-oriented actors (including privacy activists and national DPAs) without such an access can only exert indirect influence.[1213] And many actors assumed that an adequacy decision rendered by the Commission was binding and not subject to any legal scrutiny.[1214] This judgement drastically changed the power relationship among these actors.

By anchoring the adequacy requirements in EU constitutional law, *Schrems I* made it clear that the ECJ has the ultimate authority to evaluate the validity of these adequacy decisions according to the EU Charter.[1215] With the ECJ serving a "gatekeeping" role prioritizing data protection and privacy as fundamental rights, this constitutional check-and-balance structure makes it difficult for the Commission to make trade-offs that water down EU data protection during international negotiations, reining in its preference to reach deals with external trading partners out of pragmatic, economic considerations.[1216] When negotiating a successor agreement with the U.S., the Commission can no longer assume that personal data transfers for commercial purposes are separate and distinct from foreign intelligence surveillance. Instead, EU negotiators are obliged to establish safeguards, limitations, and legal remedies for EU data subjects against U.S. authorities' access of their personal data for national security purposes.

Moreover, as clarified by this ruling, the Commission's adequacy decision cannot restrict the powers of national DPAs to launch investigations over international personal data transfers, and to impose data embargo sanctions, which are essential to ensure their independent supervisory authority, as guaranteed by the EU Charter.[1217] As such, this judgment further empowered EU actors devoted to insulating EU data protection rules from American digital giants' business

[1209] *Id*., para. 103.
[1210] *Id*., paras. 102, 104-5.
[1211] Schwartz, *supra* (The EU Way), at 801.
[1212] FARRELL & NEWMAN, *supra*, at 150.
[1213] *Id*.
[1214] *Id*.
[1215] *Id*. Schwartz, *supra* (The EU Way), at 801.
[1216] See *supra* chapter ("A Battle of Big Three").
[1217] *Schrems I*, paras. 99, 103-4. See EU Charter, art. 8(3).

practices and U.S. surveillance. For privacy activists and activist DPAs, they were then able to challenge the legitimacy of the Commission's adequacy determinations before EU judiciaries sympathetic to data privacy concerns and entrusted to safeguard fundamental rights.[1218]

Second, this judicial decision emboldened the EU's position in its bilateral negotiations with the U.S. to reform Safe Harbor.[1219] Bound by its internal constitutional constraint,[1220] the EU is obliged to satisfy the ECJ's normative concerns to safeguard high-standard personal data and privacy protection as fundamental rights. With the Court voicing such normative concerns in almost non-negotiable terms, *Schrems I* indeed strengthened the Commission's bargaining powers with the U.S. negotiators.

Moreover, by articulating its expectations for a new EU-U.S. agreement post-*Schrems*, the ECJ not only provided a roadmap for EU negotiators to follow, but also made a modestly revised Safe Harbor politically and legally infeasible.[1221] As the ruling criticized at length the Safe Harbor's loopholes stemming from national security exceptions, the Court seemed to require a drastic change in how U.S. intelligence and surveillance treated Europeans' data, calling for such practices to conform with EU standards on accountability and transparency.[1222] To ensure unhindered transatlantic data flows, the Commission was thus *pressured* and *empowered* to negotiate stronger institutional safeguards to better protect EU citizens' data, lest a new deal might be struck down again by the Court.

Third, *Schrems I* broke new ground by integrating national security safeguards against foreign intelligence surveillance into EU-U.S. transatlantic data privacy norms. Previously, the Safe Harbor principles exempted information sharing necessary for national security, intelligence surveillance, or law enforcement purposes, or as required by domestic law or explicit authorizations—without precise rules disciplining the scope and application thereof, or providing minimum safeguards against potential abuses and misuses.[1223] As held by the Court, this exemption must not prevail over European data protection law, but instead must respect the essence of the fundamental rights with respect to data and privacy protection under the EU Charter.[1224] In this sense, this judgment strengthened the Court's judicial scrutiny over acceptable exemptions for national security purposes, creating additional hurdles for U.S. intelligence sharing through the Safe Harbor.[1225]

As a result, the U.S. was required to ensure essentially equivalent protection that limits interference with Europeans' fundamental rights and provides effective legal redress against such interference.[1226] In particular, the Court stressed that under the Safe Harbor, any derogations or limitations on the fundamental rights to data protection and privacy at the EU level must be strictly necessary and proportionate to competing legitimate objectives (such as protection of national

[1218] FARRELL & NEWMAN, *supra*, at 150.
[1219] Schwartz, *supra* (The EU Way), at 801. Id., at 152.
[1220] Yakoleva, *supra* (Privacy Protection(ism)), at 466.
[1221] Schwartz, *supra* (The EU Way), at 800-1.
[1222] FARRELL & NEWMAN, *supra*, at 152.
[1223] Safe Harbor Decision, *supra*, at 10, Annex I.
[1224] *Schrems I*, paras. 86-7.
[1225] FARRELL & NEWMAN, *supra*, at 149-150.
[1226] *Schrems I*, paras. 88-9.

security).[1227] Likewise, the Safe Harbor arrangement shall provide data subjects with sufficient legal remedies in regards to their data, in order to respect the essence of the fundamental right to effective judicial protection under the Charter.[1228]

B. The Privacy Shield Agreement and the ECJ Decision of Schrems II

As the ECJ invalidated the Safe Harbor and put transatlantic data transfers at high risks, the U.S. was, again, forced to negotiate an international agreement to level up data privacy standards, and particularly, to make new institutional commitments to provide national security safeguards for EU personal data. Such dynamics resulted in the Privacy Shield agreement, characterized by significant changes on data protection that would not have been politically viable without the *Schrems I* decision.

However, this new deal cannot fully assuage the normative concerns of the EU data privacy community. Building on the precedent of *Schrems I*, privacy activists and national DPAs started another round of legal actions to challenge the legitimacy of transatlantic data transfer mechanisms under EU law. This time, the subject matter of these proceedings was the SCCs and Privacy Shield, yet what was essentially on trial was still U.S. surveillance law.[1229] Again, the ECJ stepped in to scrutinize the Commission's adequacy determinations, seizing on the normative conflicts between EU data privacy rules and U.S. surveillance law to redefine the legal and regulatory requirements for transatlantic data transfers.

(A) The Privacy Shield

As the major institutional framework for transatlantic data transfers was voided, U.S. companies faced more costly, complicated, and burdensome contractual mechanisms (SCCs and BCRs). Faced with considerable legal uncertainty created by *Schrems I* for transatlantic commercial flows, [1230] the U.S. stepped up negotiations with the Commission, in efforts to safeguard transatlantic data flows essential for U.S.-EU commercial exchanges. On the EU side, Commission officials demanded stronger U.S. commitments to level up data protection, and made it clear that a deal that tackled only commercial aspects of data transfers but bracketed national security questions was politically impossible.[1231] While European DPA (i.e., the WP29) agreed not to prosecute U.S. firms that continued to use Safe Harbor until January 31, 2016, this stance effectively set a deadline for U.S. and EU negotiators to revise the agreement.[1232] In February, both sides announced their successful negotiations of a replacement deal, the Privacy Shield

[1227] *Id*., paras. 90-2.
[1228] *Id*., para. 95. See EU Charter, art. 47.
[1229] Anupam Chander, *Is Data Localization A Solution for Schrems II?*, 23 J. INT'L ECO. L. 771, 773 (2020) ["JIEL"].
[1230] WEISS & ARCHICK, *supra*, at 8 (noting that after *Schrems I*, Article 29 Working Party reaffirmed that data transfers under the Safe Harbor agreement were now unlawful and expressed broad concerns about the implications of the judgment for SCCs and BCRs).
[1231] FARRELL & NEWMAN, *supra*, at 152.
[1232] WEISS & ARCHICK, *supra*, at 8.

agreement, which was later approved by the Parliament in July and came into force in August.[1233] In July 2016, the Commission rendered an adequacy decision for the Privacy Shield agreement.[1234]

Overall, the Privacy Shield continues the basic self-regulatory framework of the Safe Harbor, but strengthens data privacy principles and oversight mechanisms in notable ways. To begin with, this agreement adopts the same principles as provided in the Safe Harbor, while enhancing participating companies' commitments to protect EU citizens' data. Specifically, the Privacy Shield creates more detailed notice obligations, enhances individuals' right to access, tightens the limits on consent as a basis for data processing, sets stricter data retention limits, reinforces data integrity and purpose limitation principles, and strengthens the security requirements.[1235]

In particular, Privacy Shield makes substantial changes to the Safe Harbor principle of "enforcement" (which is reconfigured as "recourse, enforcement and liability").[1236] Under this revised principle, participating firms must provide independent recourse mechanisms to expeditiously address data subjects' complaints and disputes at no cost to such individuals, and are obliged to expeditiously handle complaints on compliance with the principles referred by EU national DPAs through the Department of Commerce.[1237] For onward transfers of EU data, a U.S. company must assume liability for a third party agent who processes such data on its behalf in ways violative of the principles.[1238] Moreover, the Privacy Shield provides an additional set of supplemental principles, including provisions for sensitive data, human resources data, pharmaceutical and medical products, among others.[1239]

Aside from these revisions to data protection principles, the Privacy Shield also strengthens the monitoring and enforcement mechanisms to ensure compliance and accountability. Under this arrangement, the U.S. Department of Commerce would oversee compliance pursuant to FTC enforcement, with sanctions powers reinforced.[1240] Also, the Privacy Shield has broadened new redress mechanisms. Under this arrangement, EU data subjects could file complaints directly to companies, or to EU national DPAs to resolve disputes (which may refer unresolved complaints to the FTC); and alternatively, may invoke a binding arbitration procedure to address unresolved claims against such companies.[1241]

[1233] Schwartz, *supra* (The EU Way), at 802.
[1234] Commission Implementing Decision (EU) 2016/1250, of 12 July 2016, Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, Annex A (EU-U.S. Privacy Shield Ombudsperson Mechanism), at 3, para. 13, 2016 O.J. (L207) ["Privacy Shield Decision"].
[1235] U.S. Department of Commerce, EU-U.S. Privacy Shield Framework Principles, Section II.7 (principle of "recourse, enforcement and liability"), Sections II to III, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg ["EU-U.S. Privacy Shield Framework Principles"]. WEISS & ARCHICK, *supra*, at 10.
[1236] EU-U.S. Privacy Shield Framework Principles, *supra*, Section II.7 (principle of "recourse, enforcement and liability"). Compare with Safe Harbor Decision, at 12 (principle of "enforcement").
[1237] *Id*.
[1238] *Id*.
[1239] *Id*., at Section III.
[1240] WEISS & ARCHICK, *supra*, at 10 (in extreme cases, a non-compliant company may lose its eligibility to use the Privacy Shield to transfer EU data).
[1241] *Id*.

As for complaints on U.S. intelligence agencies' surveillance of EU citizens' data, a new specialized ombudsperson is established in the U.S. Department of State to monitor and oversee such matters.[1242] Independent of the U.S. intelligence community, the ombudsperson is mandated to review issues and complaints referred by a EU centralized body.[1243] Moreover, the Office of the Director of National Intelligence has provided written assurances that the U.S. intelligence apparatus would not conduct indiscriminate mass surveillance on EU citizens' data transferred under the Privacy Shield, and that its access to such data are subject to limitations, safeguards, and oversight mechanisms under U.S. law.[1244]

Finally, on the EU side, the Commission establishes new review mechanisms to periodically check whether its adequacy finding on the Privacy Shield is still factually and legally justified.[1245]

In short, through *Schrems I*, the constitutionalization of the EU's adequacy standard has empowered the Commission to successfully bargain for greater concessions from the U.S. than what would otherwise be politically possible. This enables the new transatlantic data transfer agreement to substantially ramp up substantive data protection principles, monitoring and oversight mechanisms, and national security safeguards.

(B) The ECJ's Decision of *Schrems II*

While the Privacy Shield has considerably enhanced data protection safeguards of the Safe Harbor, the European data privacy community was still less enthused about this agreement. In April 2016, the WP29 issued an opinion on the deficiencies of the Privacy Shield agreement.[1246] Though recognizing "major improvements" made by this instrument, this opinion expressed strong concerns over its key *commercial* and *national security* aspects.[1247] Regarding the former, the WP29 criticized, for example, the lack of some EU data protection principles (such as an explicit data retention principle, protection against algorithmic decision-making), insufficient protection for onward transfers of EU citizens' data, and overly complex redress mechanisms.[1248] As for the latter, this opinion emphasized that the commitments of the U.S. Office of the Director of National Intelligence cannot fully exclude indiscriminate mass surveillance.[1249] It also questioned the ombudsperson mechanism's independence, as well as its powers to guarantee an effective legal remedy under EU law.[1250] In conclusion, the WP29 called on the Commission to resolve these concerns and improve data protection.[1251] Echoing such normative concerns, the European Data

[1242] Privacy Shield Decision, at 72-7.
[1243] *Id*.
[1244] *Id*., at 103-4, Annex VI (Letter from Robert S. Litt, General Counsel of Office of the Director of National Intelligence, to Justin S. Antonipillai, Counsellor of U.S. Department of Commerce, and Ted Dean, Deputy Assistant Secretary of International Trade Administration, dated February 22, 2016).
[1245] *Id*., at 33, para. 145 (periodic review of adequacy finding).
[1246] Article 29 Working Party, Opinion 01/2016 on the EU—U.S. Privacy Shield Draft Adequacy Decision, WP 238 (adopted on April 13, 2016), https://www.pdpjournals.com/docs/88536.pdf.
[1247] *Id*., at 3-5.
[1248] *Id*., at 3, 33. The lack of an explicit data retention principle means that the Privacy Shield contains no clear obligation on U.S. organizations to delete EU citizens' personal data once no longer necessary for the original purpose for which they were collected.
[1249] *Id*., at 4.
[1250] *Id*.
[1251] *Id*., at 5.

Protection Supervisor (the EU's DPA) likewise argued that the Privacy Shield was not "robust enough to withstand future legal scrutiny" of the ECJ.[1252] Rather, it urged the Commission to make "significant improvements" to "respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms".[1253]

In parallel, EU privacy activists stepped up legal campaigns to challenge the Privacy Shield, in efforts to protect EU citizens' data transferred to the U.S. In September 2016, Digital Rights Ireland, an NGO devoted to individuals' internet freedom, brought a legal action to the ECJ, challenging the legality of the Commission's adequacy decision on the Privacy Shield.[1254] But this action was unsuccessful, as the Court found that the applicant lacked the standing to sue.[1255] In October 2016, La Quadrature du Net, a French advocacy group applying to intervene in support of Digital Rights Ireland, also initiated its own legal action before the ECJ, requesting the Court to annul the Privacy Shield for violations of fundamental rights under the EU Charter.[1256] Among such legal actions, the most successful one was the claims brought by Irish data protection commissioner in response to Schrems' complaint.

Following the ECJ judgment of *Schrems I*, Facebook Ireland Ltd. asserted that it transferred, in large part, EU personal data to its U.S. headquarters through the SCCs, which received adequacy decisions from the Commission.[1257] In December 2015, through a reformulated complaint before the Irish DPA, Schrems challenged the validity of Facebook's use of the SCCs, arguing that U.S. intelligence authorities' access to his data for national security purposes violated his fundamental rights under the EU Charter (i.e., the rights to privacy, personal data protection, and an effective legal remedy).[1258] The Irish DPA rendered a draft decision, provisionally finding that the SCCs used by Facebook cannot adequately protect EU citizens' data against U.S. intelligence surveillance.[1259] Relying on the ECJ ruling of *Schrems I*,[1260] that DPA brought a legal action to the Irish High Court, challenging the validity of the Commission's adequacy decision over the SCCs.[1261] The High Court, after finding that U.S. surveillance law permitted mass surveillance of personal data transferred from the EU, referred to the ECJ eleven questions over the legality of transatlantic data transfers.[1262] These include (i) whether transfers of Europeans' data under the SCCs to the U.S. violated fundamental rights under the EU Charter, (ii) whether the Commission's

[1252] European Data Protection Supervisor, *Privacy Shield: More Robust and Sustainable Solution Needed*, PRESS RELEASE (May 30, 2016), https://edps.europa.eu/press-publications/press-news/press-releases/2016/privacy-shield-more-robust-and-sustainable_en.
[1253] *Id.*
[1254] See Case T-670/16, *Digital Rights Ireland Ltd. v. Commission*, ECLI:EU:T:2017:838.
[1255] *Id*.
[1256] Case T-738/16, *La Quadrature du Net and Others v. Commission*, Order (OJ), January 29, 2021.
[1257] *Schrems II*, para. 54.
[1258] *Id*., para. 55. Schrems requested the DPA to "prohibit or suspend the transfer of his personal data to Facebook Inc." See *id.*
[1259] *Id.*, para. 56 (the Commissioner concluded with the provisional view that EU citizens' personal data transferred to the U.S. may be accessed by U.S. authorities without providing those individuals with effective legal remedies, violative of the fundamental rights under the Charter; and that this legal deficiency cannot be remedied by SCCs, which, as a contractual mechanism, cannot bind U.S. authorities).
[1260] *Schrems I*, para. 65 (stating that if national DPA deems an EU data subject's complaint well founded, it must initiate legal actions before national court to challenge the Commission's adequacy decision, which may refer the issue to the ECJ for a determination).
[1261] *Schrems II*, para. 57.
[1262] *Id*., para. 68.

adequacy decision for the Privacy Shield was binding on national DPAs and the courts of EU member states, and (iii) whether the Privacy Shield ombudsperson system provided an effective remedy against U.S. intelligence surveillance.[1263]

In July 2020, the ECJ rendered another landmark judgment that, once again, substantially influenced transatlantic privacy lawmaking and complicated data transfer practices—*Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* ("*Schrems II*"). In this decision, the Court invalidated the EU-U.S. Privacy Shield agreement,[1264] which had been used by over 5,300 U.S. and EU companies to transfer personal data across the Atlantic.[1265] In addition, the Court upheld the legality of the SCCs (that a large portion of data exports from the EU reply on),[1266] meanwhile imposing stricter requirements for SCC-based data transfers.[1267]

As regards the Privacy Shield, the Court found that U.S. surveillance law authorizing and regulating intelligence surveillance failed to provide adequate protection for EU data subjects as required by the EU Charter and GDPR.[1268] As held by the Court, Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12,333—as the U.S. legal bases for surveillance programmes (such as PRISM, UPSTREAM)—were unduly broad and lacked sufficient legal redress mechanisms for EU data subjects, violative of their fundamental rights under the Charter.[1269] In breach of the principle of proportionality, such surveillance law does not sufficiently limit the powers of U.S. authorities to implement surveillance programmes "to what is strictly necessary", constituting disproportionate interference with the rights to privacy and data protection under the EU Charter.[1270] On the other hand, U.S. law does not provide for actionable rights for EU data subjects in the courts against U.S. authorities to access their data and have them rectified or erased, and thus violates the fundamental right to an effective legal remedy under the EU Charter.[1271] Neither can the Privacy Shield ombudsperson effectively remedy such deficiencies of judicial protection, as that mechanism itself lacks complete independence from the executive, as well as sufficient powers to provide a cause of action for EU data subjects (or to adopt binding decisions on intelligence services).[1272] As a result, the Court concluded that the Privacy Shield cannot guarantee a level of protection essentially equivalent to the GDPR and EU Charter.[1273]

Moreover, while finding the SCCs as a valid data transfer mechanism under EU law, the Court imposed strengthened monitoring and oversight responsibilities on data processors and supervisory authorities to ensure an adequate level of protection.[1274] To that end, it firstly required data exporters and recipients to verify, prior to any transfer, whether a third country ensured the level of protection required under EU law.[1275] Where necessary (e.g., the SCCs cannot bind U.S.

[1263] *Id*.
[1264] *Id*., paras. 198-201.
[1265] Chander, *supra* (JIEL), at 773.
[1266] *Id*., at 774.
[1267] *Schrems II*, paras. 133-5, 148-9.
[1268] *Id*., paras. 198-201.
[1269] *Id*., paras. 184, 192.
[1270] *Id*., paras. 180-5.
[1271] *Id*., paras. 181-2, 191-2.
[1272] *Id*., paras. 190, 194-7.
[1273] *Id*., para. 198.
[1274] *Id*., paras 133-5, 149.
[1275] *Id*., paras. 134, 142.

public authorities conducting intelligence surveillance), data controllers and processors must adopt "supplementary measures" (though undefined) to compensate for the lack of data protection in a third country's legal system.[1276] Failing that, data operators must suspend or terminate transfers of EU citizens' data to that country.[1277] Meanwhile, the Court required EU national DPAs to suspend or prohibit such transfers, if "in light of all the circumstances" the SCCs-based transfers cannot provide adequate level of protection in a third country.[1278]

Following *Schrems I*, this judgment raises a higher threshold for achieving an "adequacy" decision, demanding more stringent conditions on data protection for a third country and data processing firms to comply with. Building on *Schrems I* that held that commercial data transfers must be warded off from intelligence surveillance, the Court further narrowed acceptable exemptions to data protection arising from U.S. surveillance law, tightening its judicial review over U.S. authorities' access and use of EU citizens' data for national security purposes. While the Privacy Shield indeed incorporated improved national security safeguards and oversight mechanisms, the *Schrems II* decision considered such initiatives not sufficient to ensure a level of protection "essentially equivalent to" the EU law. To achieve an "adequacy" status, the Court demands even stronger institutional commitments, safeguards, and legal remedies from U.S. intelligence services, and beyond, to strictly limit the government's powers to implement surveillance programmes against EU data subjects to the extent necessary, and to provide for actionable rights before U.S. courts to effectively enforce their individual rights—as guaranteed by their fundamental rights under the EU Charter. Following the collapse of the Privacy Shield, this judgment *obliges* and further *empowers* the Commission to negotiate another agreement with the U.S. for transatlantic data transfers, enabling the EU to push for more robust and comprehensive data protection rules and more effective enforcement and oversight mechanisms—including commercial data protections and national security safeguards.

Further, this ruling considerably strengthens the regulatory scrutiny over SCCs-based data transfers to the U.S. and beyond. Essentially, it turns all SCCs into "mini adequacy decisions" at an organizational level,[1279] as it obliged all data operators to verify themselves whether a data transfer can properly proceed based on the available level of data protection in a third country. To ensure unrestricted international data flows, companies processing EU citizens' data must adopt additional safeguard measures to protect against possible loopholes and lacunae in a third country's legal system. To be sure, this is not to move towards a U.S.-styled hands-off, self-regulatory regime. Rather, such a reinforced corporate compliance responsibility is keenly overseen by the GDPR's robust enforcement and oversight mechanisms (featuring considerable data embargo powers and sanctions) and the EU's highest court, closely monitoring companies' behavior while obtaining their participation in determining how fundamental rights are protected in specific contexts.[1280]

[1276] *Id*., paras. 133-4.
[1277] *Id*., para. 135.
[1278] *Id*., paras. 121, 134-5.
[1279] Christopher Kuner, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUROPEAN LAW BLOG (July 12, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/.
[1280] See Kaminski and Jones, *supra*, at 119; Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV 1529, 1615 (2019).

For critics, this judgment's treatment of the SCCs (in demanding "supplementary measures" without explaining in detail what that can or should be) generates huge legal uncertainty and vastly complicates transatlantic data transfers, adding to companies' compliance costs and legal fees to stay safe from EU regulators. For smaller firms, this new normal may well goad them away from data exporting, but instead incentivizes them to store and process EU citizens' data within Europe to ensure compliance, constituting a soft version of "data localization" for data privacy protection purposes.[1281]

Moreover, *Schrems II* continues the trend of constitutionalizing the adequacy standard, further empowering activist EU national DPAs and privacy activists to scrutinize transatlantic data flows. Under this ruling, EU national data privacy commissioners can wield considerable powers to check on U.S. firms' data processing policies and practices, as they can conduct regulatory and enforcement actions at their discretion against SCC-based data transfers. As expert actors with delegated authority, DPAs at the EU and member state levels are mandated with interpreting what the appropriate "supplementary measures" should be, and monitoring the implementation of this new requirement. Immediately after *Schrems II*, the Berlin German DPA threatened to block data transfers under the SCCs to the U.S., should the U.S. government have access to personal data transferred thereunder beyond the limits of EU law.[1282] Likewise, the Portuguese data privacy commissioner, in April 2021, ordered an organization to suspend SCCs-based transfers of personal data to the U.S., as it considered that the recipient entity was bound by U.S. surveillance law to provide U.S. authorities with unrestricted access to those data without securing adequate protection.[1283]

In addition, EU privacy activists, like Schrems, are further empowered to double down on their cause of guarding EU data protection law against external pressures. Relying on this precedent (and *Schrems I*), privacy advocates could target other transatlantic data transfer mechanisms, including a successor deal, other "alternative safeguards" (e.g., BCRs, certifications), and the U.S.-EU Passenger Name Records (PNR) and SWIFT agreements.[1284] By bringing complaints before national DPAs and launching legal actions before EU courts, these activists may well start another round of regulatory and legal change to further ratchet up transatlantic data privacy protection and to remedy any potential loopholes thereof.

C. Implications for International Transfers of Personal Data

[1281] Chander, *supra* (JIEL), at 777-8.

[1282] *Berlin: Berlin Commissioner Issues Statement on Schrems II Case, Asks Controllers to Stop Data Transfers to the US*, https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data.

[1283] Portuguese DPA Orders Suspension of U.S. Data Transfers by Agency That Relied on SCCs, April 28, 2021, https://www.huntonprivacyblog.com/2021/04/28/portuguese-dpa-orders-suspension-of-u-s-data-transfers-by-agency-that-relied-on-sccs/.

[1284] The U.S.-EU PNR agreement is an international agreement to provide passenger name records from EU-based air carriers operating passenger flights to the U.S. Department of Homeland Security for national security and public security purposes. See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012AP0134&rid=9; The U.S.-EU SWIFT agreement is an international agreement for U.S. authorities to gain access to SWIFT financial data for counterterrorism purposes. See https://www.statewatch.org/media/documents/news/2010/jun/eu-usa-draft-swift-agreement-com-final-2.pdf. Both agreements received an "adequacy" decision from the Commission. See KUNER, *supra*, at 41.

As shown in the above cases, the EU data privacy regime generates two major implications for international personal data transfers from the EU to the U.S. and other countries.

First, under its regulatory approach to cross-border personal data transfers, the EU obtains significant leverage to require its trading partners to level up data protection standards and converge on EU data privacy norms. By controlling access to its single market, the EU pressured the U.S. to negotiate the Safe Harbor and Privacy Shield agreements to permit unrestricted transatlantic data transfers. Participating U.S. firms are thus obliged to comply with EU data privacy principles and are subject to regulatory and enforcement actions launched by national DPAs in Europe. As such, even the U.S.—one of the few major holdouts rejecting a comprehensive data privacy regime—has adapted to EU standards in unique ways.[1285]

Given that the EU is one of the world's largest markets with more than 500 million consumers, its other trading partners that do not wish to obstruct digital trade flows with Europe, likewise, are pressured to obtain adequacy decisions from the EU.[1286] As noted by Newman, "[j]ust as national data privacy authorities had threatened to block data transfers between European countries in the late 1980s, under the directive (and the GDPR) the European Union now had the authority to stop cross-border exchanges between Europe and other nations."[1287] This confers the EU with significant bargaining power during its adequacy discussions and negotiations. By this virtue, the EU could demand these third countries to reform their domestic data protection laws (or to provide enforceable international commitments), in order to ratchet up data privacy standards to a level that satisfied the EU.[1288] Under the rulings of *Schrems I* and *II*, foreign legislators and regulators are even more pressured to closely follow EU data privacy rules, in efforts to obtain an adequacy decision that can withstand the ECJ's scrutiny. In this way, the EU could advance its data privacy norms globally, pressuring foreign jurisdictions and companies to follow European data privacy standards worldwide.[1289] Indeed, since the mid-1990s when the Directive was enacted, EU data privacy norms have increasingly become the *de facto* international standards for many countries—a trend that continues up until the present, and which has accelerated after the adoption of the GDPR.[1290]

Second, the constitutionalization of data protection and privacy enables the ECJ to engage in pro-fundamental-rights judicial lawmaking, moving the ultimate legal authority to control the adequacy determinations from the Commission to the Court. By constitutionalizing the EU's adequacy standard, this forum-shifting process considerably empowers EU privacy advocates and activist DPAs to protect Europeans' data, at the expense of the Commission that may have

---

[1285] NEWMAN, *supra*, at 111.
[1286] Scott and Cerulus, *supra* ("Breaking commercial ties with the world's largest trading bloc is unthinkable… 'Any country that's not working toward (EU data privacy) standards is left out in the cold'.").
[1287] NEWMAN, *supra*, at 103.
[1288] Schwartz, *supra* (The EU Way), at 774.
[1289] Scott and Cerulus, *supra* (quoting John Bowman, the former lead negotiator for the U.K. on EU data privacy rules: "Europe wanted to be seen selling a global standard… That's crystallized through its adequacy decisions").
[1290] NEWMAN, *supra*, at 36-7, 102-111; Graham Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/2022 (March 15, 2022)*, 176 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORTS 1, 1-9 (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4137418 (noting that by mid-March 2022, a total of 157 countries have enacted national data privacy law, and "most of these laws are influenced substantially by the EU's GDPR"; that "the EU GDPR (incorporating its predecessor, the 1995 DPD) is clearly the *global template* on which most other countries new laws are based…. ").

preferred to make deals with the U.S. to facilitate transatlantic commercial flows.[1291] On the one hand, the ECJ's judicial decisions enable these activists and DPAs to challenge the Commission's adequacy findings before EU judiciaries highly sympathetic to privacy and human rights concerns, making it far easier to insulate EU data privacy rules from external pressures and to limit and disrupt transatlantic data-sharing agreements.[1292] By linking commercial data transfers and foreign intelligence surveillance (as exposed by the Snowden revelations), these civil-liberties-oriented actors and institutions have initiated different rounds of legal campaigns to seek regulatory change, vigorously scrutinizing the validity of transatlantic data transfer mechanisms under the EU law (including the Directive/GDPR and the EU Charter) before EU courts.

On the other hand, through forum-shifting, the ECJ has asserted dominance in determining the legitimacy of the Commission's adequacy decisions for international data transfers, obliging the Commission, EU trading partners, and data processors to satisfy its high-standard requirements to sufficiently protect Europeans' data privacy against private business practices and foreign intelligence laws. As a result, this demands that the Commission negotiate better deals with improved institutional safeguards for EU personal data, and raises the bar for alternative transfer mechanisms (such as the SCCs and BCRs). Meanwhile, the ECJ also bolsters the bargaining position of EU negotiators, and thus enables them to overcome the political difficulties to obtain stronger concessions from the U.S. (and other states with similar surveillance laws and practices), better insulating EU-originated personal data from foreign intelligence surveillance for national security purposes.

V. CONCLUSION

Through the analytical lens of forum-shifting, this chapter explains the formation and development of EU data protection regulation. Specifically, it explored three concrete rule-making processes, whereby different, though partially overlapping, institutional actors deployed the strategy of forum-shifting to shape European data privacy lawmaking on their preferred terms. By tracing the dynamic processes of supranational rulemaking, this work charts the institutional trajectory through which the EU data privacy regime came into being.

First, from the 1980s to the mid-1990s, with the establishment of more national DPAs, a coalition of these institutional actors moved the thrust of regional data privacy lawmaking from a multilateral convention to the EU's unilateral legislative acts. While one of the most influential international treaties to regulate data privacy, the Convention 108 contained many gaps and limitations, and did not stimulate the enactment of national data protection laws in many EU member states, failing to adequately harmonize domestic regulations across Europe. Dissatisfied with this institutional status quo, national DPAs turned to the Commission to pursue their policy preferences, pushing for a comprehensive set of high-standard data privacy rules. Acting in concert at the EU level, these actors built issue-linkages between data privacy protection and European market integration, leveraged their data embargo powers to alter the regulatory status quo for core EU policymakers of inaction, and deployed their expertise and network ties to shape the content of the legislative proposal. As a result, the EU Data Protection Directive was adopted, substantially changing the regulatory framework. Manifesting an upward harmonization of regulatory standards,

[1291] FARRELL & NEWMAN, *supra*, at 158.
[1292] *Id*., at 150, 158.

the Directive required member states to implement omnibus, strict national data protection laws to ensure an equivalent level of protection and to facilitate cross-border data flows across Europe.

Second, since the enactment of the Directive, a powerful group of rights-oriented institutional actors (including the WP29, ECJ, ECtHR, and DG Just) continuously sought to elevate the legal status of data privacy protection under EU law and to revamp European data protection regulation. These efforts could be grouped into two concrete stages.

In stage one, the WP29 played an instrumental role in the constitutionalization of data privacy protection in Europe, enshrining the rights to privacy and data protection into EU primary law. Such initiatives were supported and endorsed by the judicial lawmaking of two trustees of the European constitutional order—the ECJ and ECtHR. The constitutional underpinnings of data privacy protection bolstered the protective standards for data privacy, and created a new legal basis to reform EU data protection law.

In stage two, the DG Just, seizing the resultant institutional opening, became the lead DG within the Commission to govern data protection reform, and has had successfully pushed through a new legislation to revamp existing EU regulatory framework. Teaming up with the DG Just, the WP29 exerted an outsized influence in shaping the content of the proposed regulation, the GDPR. Using the Directive as a baseline, the GDPR further levels up the protection of data privacy (through reinforced individual rights and corporate compliance duties), strengthens the enforcement and oversight mechanisms, and improves the regulation of cross-border personal data flows.

Third, the constitutionalization of data privacy protection opens a new institutional route for European courts to examine the legality of international data transfer mechanisms under the EU Charter. In the aftermath of Snowden revelations, the ECJ pursued pro-fundamental-rights judicial lawmaking, vigorously scrutinizing the Commission's adequacy decisions with the U.S. Through the judgments of *Schrem I* and *II*, the Court has shifted the ultimate legal authority to control the EU's adequacy determinations from the Commission to itself, asserting dominance in deciding the legal and regulatory requirements for transferring personal data outside Europe. By constitutionalizing the "adequacy" standard, the Court pressured the Commission, EU trading partners, and private firms alike to remedy potential regulatory loopholes, meanwhile leveling up protection of EU personal data against corporate practices and foreign intelligence surveillance. Further, the ECJ's rulings empowered privacy activists and national DPAs to challenge international data transfer mechanisms before national and EU courts, strengthening the scrutiny over the Commission's adequacy findings. Collectively, the ECJ's forum-shifting initiatives may have set in motion an almost irreversible cycle for DPAs, activists, and the Commission to continuously ratchet up the protection for EU citizens' data transferred across the Atlantic and beyond, based on the Court's strong preference for high-standard protection of fundamental rights.

As a result of these major lawmaking processes, the EU data privacy regime came into shape and evolved over time. From the Directive to the GDPR, the EU has established a comprehensive data protection framework, characterized by high-standard data privacy principles, robust individual rights, and strong enforcement and oversight. While these legislations constitute the institutional backbones of European data protection regulation, they only establish a floor, rather than a ceiling, since they are supplemented by sector-specific regulations and other legal sources. Further, the EU

data privacy regime protects personal data and privacy as fundamental rights, establishing the primacy of data privacy over the economic interests underlying personal data by default. While the EU also promotes personal data flows across national borders, such transfers depend on the satisfaction of the adequacy standard, which is actively scrutinized by the ECJ. To maintain unrestricted data transfers essential for trade flows with Europe's market, foreign jurisdictions are required to ensure essentially equivalent protection for EU data subjects, and thus are pressured to converge their data privacy laws on EU standards.

As with two sides of the same coin, high-standard data privacy protection and the adequacy approach to transnational data flows are inseparable from each other. Stringent data privacy standards not only demand the EU to extend its fundamental rights paradigm abroad to protect Europeans' data transferred outside Europe, but also provide a benchmark to evaluate whether a foreign legal system ensures an adequate level of data protection. The adequacy requirements also serve to remedy potential regulatory loopholes by preventing foreign "data havens" from undermining EU rules. Meanwhile, by controlling the access to Europe's single market, the adequacy standard pressures foreign regulators and firms to follow EU data protection norms, enabling the EU to externalize its data privacy standards worldwide. Combined, these two core components of the EU's regulatory approach allow the EU to become a global leader on data privacy lawmaking. At a time when other superpowers (the U.S. and China) have been advancing their preferred governance models to regulate cross-border data flows,[1293] the EU data privacy regime empowers the EU to make a powerful claim to determine the terms and conditions for data privacy protection and international personal data transfers.

Appendix

Table: How the EU's forum-shifting has shaped the European data privacy regime

[1293] See *supra* chapter (Three Conceptualizations); Aaronson & Leblond, *supra*, at 268-9.

	Vertical Forum Shifting 1.0	Vertical Forum Shifting 2.1	Vertical Forum Shifting 2.2	ECJ-led forum shifting
Timing	From the 1980s to the mid-1990s	From the mid-1990s to 2012	From the mid-1990s to 2016	From 2013 (Snowden revelations) to present
Principal actors (or coalition)	EU national DPAs	Article 29 Working Party, ECJ, ECtHR	DG JUST, Article 29 Working Party, national DPAs	ECJ and its allies (Irish High Court, Irish DPA, privacy activists like Shcrems)
Challenged institutions/rules	Convention 108	That data protection and privacy were only protected by EU secondary law	EU Data Protection Directive	The Commission's adequacy decisions on the Safe Harbor, Privacy Shield, SCCs
Primary sources of dissatisfaction	Endogenous: EU member states' divergent data privacy laws, which was not sufficiently addressed by the Convention 108	Endogenous: pressure from Article 29 Working Party; the ECJ and ECtHR's rights-activism judicial lawmaking	Endogenous (primary): pressure from DG Just, Article 29 Working Party, national DPAs; Exogenous (supplementary): Snowden revelations, highlighting issue-salience of data privacy protection	Exogenous: U.S. surveillance law
Major reversion points	Threatening to block internal European market integration	N.A.	N.A.	Threatening to block transatlantic data transfers
New rules or institutional outcomes	**EU Data Protection Directive**	**EU Charter of Fundamental Rights** (articles 7-8); **Treaty on the Functioning of the EU** (article 16)	**GDPR**	***Schrems I, Schrems II***
Institutional outcomes	The Directive came into effect: - high-standard regulatory controls over data processing; - a qualified prohibition approach to cross-border personal data transfers; - establishing DPAs and formalizing their transgovernmental network	The constitutionalization of data privacy protection: - enshrining the rights to privacy and data protection as fundamental rights under EU primary law; - empowering civil-liberties-oriented actors within the Commission to push through the GDPR to reform the Directive; - enabling the ECJ's pro-fundamental-rights judicial lawmaking over transatlantic data transfers	The GDPR replaced the Directive: - a harder law with an extended reach; - enhanced individual rights of EU data subjects; - strengthened corporate compliance responsibilities; - improved regulation on international personal data transfers; - reinforced enforcement and improved cooperation of DPAs	Pro-fundamental-rights judicial lawmaking: - constitutionalizing the Commission's adequacy standard; - pressuring and empowering the Commission to negotiate new U.S.-EU data transfer agreements with improved data privacy protection; - empowering EU privacy activists and DPAs to challenge transatlantic data transfer mechanisms before EU courts; - integrating national security safeguards into the U.S.-EU data transfer mechanisms

Chapter 4

Implications of EU Data Protection Law for the Transnational Regime Complex Governing Cross-Border Personal Data Transfers

Table of Content

INTRODUCTION **195**

I. IMPLICATIONS FOR THE INTERNATIONAL TRADE REGIME: BRACKETING AND COORDINATION **196**

A. The Privacy Bracketing in International Trade Agreements ***196***

(A) The Privacy Exception in the GATS 196

(a) The Creation of the GATS Privacy Exception *197*

(b) Implications of the GATS Privacy Exception *199*

(B) The EU's Privacy Exceptions in International Trade Agreements After the GATS 201

(a) EU-led PTAs Negotiated Before 2018 ..... *201*

(b) 2018 EU Model Exceptions *203*

B. Coordinating the EU's "Adequacy" and Trade Negotiations ***206***

II. IMPLICATIONS FOR GLOBAL DATA PRIVACY PROTECTION: EU DATA PROTECTION LAW RISING AS THE GLOBAL STANDARDS **208**

A. The Political Economy Undergirding the EU's Global Rule-Making ***209***

B. De Facto Brussels Effect Among Multinationals ***211***

C. The Spread of EU Data Privacy Law among Third Countries ***214***

(A) The Dominance of EU Data Protection Law as a Globalized Regulatory Model 214

(B) Mechanisms and Factors Driving Third Countries' Legal Transplants Worldwide 216

(a) De Jure Brussels Effect *217*

(b) The Potency of the "Adequacy" Requirements *218*

(c) Issue-Linkages *222*

(d) Accessibility and Normative Appeal of the EU Model *223*

III. CONCLUSION **225**

INTRODUCTION

Through vertical forum-shifting, EU data protection regulation comes to rise and rule the processing of personal data in Europe and beyond. Yet, the influence of this legal regime is by no means limited to regional data privacy policymaking, but increasingly spills over to shape the EU's trade law-making in the multilateral, regional, and bilateral fora. Further, EU data protection law has been increasingly diffusing beyond European jurisdictions as a regulatory model. With

increasing numbers of foreign companies and governments following such rules, EU data protection regulation emerges as a prominent set of international data privacy standards, establishing the EU's sphere of regulatory influence around many parts of the globe.

This chapter explores two case studies, manifesting the normative and policy implications of the EU data privacy regime for the transnational regime complex governing cross-border personal data flows. Part I analyzes the implications of EU data protection regulation for the EU's international trade lawmaking. Part II explores the diffusion of European data protection norms as emerging international standards among multinationals and third countries, evidencing the influence of EU rules on global data privacy protection. Part III summarizes with conclusive remarks.

I. IMPLICATIONS FOR THE INTERNATIONAL TRADE REGIME: BRACKETING AND COORDINATION

The European data privacy regime generates two significant implications for the EU's international trade agreements. On the one hand, EU data privacy law *constrains* the Commission's leeway for international trade negotiations, pressuring European negotiators to establish privacy exceptions to ensure sufficient regulatory autonomy to implement internal data protection measures. Over time, such privacy exceptions ended up in stronger terms and became easier to invoke, constituting a prominent feature of the EU's approach to digital trade. On the other hand, the EU, cognizant of the importance of its adequacy findings to foreign countries, comes to increasingly coordinate its international trade negotiations with data protection processes, and thus boosts its influence and capacity to advance EU agendas in the trade arena. In this sense, the EU's data protection regime also *empowers* European trade policymaking.

A. The Privacy Bracketing in International Trade Agreements

In the context of international trade, the European Commission enjoys centralized authority to negotiate international treaties on behalf of the entire Union.[1294] In so doing, the Commission must advance and protect common EU interests, rather than those of individual member states.[1295] With the development of EU data protection law, European trade negotiators were pressured to safeguard the EU's regulatory autonomy to adopt data protection regulation, which is essential for maintaining the integrity of the internal market and safeguarding the fundamental rights of Europeans.[1296] However, as international trade agreements move towards greater liberalization of trade in services and cross-border information flows, EU data privacy measures that restrict, and even, ban cross-border transfers of personal data increasingly risk violating such trade liberalization rules. In response, EU trade negotiators come to develop privacy exceptions in international trade agreements, designed to carve out EU data privacy measures from their disciplines. Through these provisions, the EU seeks to defend the exclusive decision-making authority of its data privacy regime to regulate cross-border data flows and personal data protection.

(A) The Privacy Exception in the GATS

[1294] ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 115 (2008).
[1295] *Id.*, at 116; BRAFORD, *supra* (BRUSSELS EFFECT), at 8-9.
[1296] NEWMAN, *supra*, at 116.

(a) The Creation of the GATS Privacy Exception

The tension between the EU's regulatory approach to international transfers of personal data and the international trade regime first surfaced in the negotiations of the General Agreement on Trade in Services (GATS). Concluded at the Uruguay Round of multilateral negotiations, the GATS expands the reach of international trade rules (which used to govern goods only) to regulate trade in services.[1297] Under this agreement, member states are obliged to provide non-discriminatory treatment—including most-favored-nation treatment and national treatment—and market access to service suppliers of other WTO member states, to the extent of their undertakings to liberalize a particular (sub-)sector.[1298] This requires signatory countries not to discriminate among foreign and domestic service providers, and to ensure that other member states are treated equally.

Such a bold progress of international trade liberalization largely reflects and serves the economic interests of the U.S. and the EU, which were the major proponents of this treaty. Indeed, during the Uruguay Round, the U.S. already perceived itself as a global leader in information services, and leading American financial service giants played an important role in lobbying for multilateral trade rules on services.[1299] Meanwhile, the EU was also a major beneficiary of free trade in services, which depended on cross-border data flows.[1300] Both economic superpowers thus would substantially benefit from multilateral trade rules to liberalize trade in services and to avoid local barriers to cross-border data flows.

However, EU data protection law may violate the GATS rules, since it distinguishes between foreign countries based on their levels of data protections, and restricts or prohibits outbound transfers of personal data (often essential to cross-border flows of trade in services) to countries deemed to have inadequate data protection laws.[1301] The question for the EU then becomes how to reconcile the normative tensions between the GATS' commitments of trade liberalization and the European regulatory approach to international personal data transfers.

When the Uruguay Round negotiations were concluded in the mid-1990s, the development of the EU Data Protection Directive also came to a final phase.[1302] With such trade and privacy initiatives running in parallel, the Commission officials correctly expected that other trading partners would raise objections to European data protection law in the 1990s, just like it had considered such rules to be a non-tariff barrier to trade in the 1980s.[1303] This led the Commission to realize the need to remove data privacy measures from the discipline of international trade rules, in order to safeguard the European data protection law which it viewed as essential for the completion of the internal

[1297] Bernard Hoekman, *The General Agreement on Trade in Services*, *in* READINGS OF THE NEW WORLD TRADING SYSTEM (OECD 1994).
[1298] See e.g. GATS, arts. II (most-favored-nation treatment), XVI (market access), and XVII (national treatment).
[1299] Chander and Schwartz, *supra*, at 13-16.
[1300] *Id.*, at 16 (noting that in 1994, the EU was more dependent on exporting trade in services than goods, and that European firms were world leaders in finance, insurance, and other professional services, like their US peers).
[1301] For a detailed doctrinal analysis, see Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH. 182, 199-205 (2017).
[1302] NEWMAN, *supra*, at 116-17.
[1303] *Id.*, at 116.

market.[1304] In fact, the Commission's negotiators went to the GATS negotiations with the goal of carving out EU data privacy rules.[1305] In June 1990, the Commission submitted a proposal to include privacy and data protection into the public policy exceptions of the GATS,[1306] whose prior proposed text contained no such mention.[1307]

On the other hand, the U.S., not fully grasping the implications of the EU's privacy exemption, raised no objection to the EU's proposal.[1308] As observed by Abraham Newman, this was due to the GATS negotiations occurring before the release of the final draft of the EU Data Protection Directive, and the US negotiators having no major official working on data privacy rules.[1309] While GATS negotiators indeed recognized that data privacy policies somehow implicated trade in services, the U.S. initially considered European data protection initiatives as largely a matter of intra-European trade, and did not sufficiently appreciate their extraterritorial effects.[1310] As a result, at the Uruguay round, the EU successfully pushed to insert a privacy exemption into the final text of the GATS, without much political resistance.[1311]

As stipulated by this provision, member states may adopt measures "necessary to secure compliance with laws or regulations", including those regarding "the protection of the privacy of individuals in relation to the processing and dissemination of personal data".[1312] To invoke this exemption, the privacy measure must be "*necessary*" to achieve the policy goal of data privacy protection. In the WTO jurisprudence, the satisfaction of this "necessity" nexus requires the absence of a "reasonable available" alternative measure that imposes a lesser burden on trade, but achieves the same policy objective.[1313] Further, as required by the chapeau clause of all GATS exceptions, the privacy measure must satisfy the *non-discrimination* requirement: it should not be applied in a manner that would constitute "a means of arbitrary or unjustifiable discrimination

---

[1304] The EU Data Protection Directive has two primary goals: to protect individuals' data privacy and to ensure free flows of personal data between EU member states (which is indispensable for achieving the EU single market). These two goals are inseparable from each other. In the 1980s, national data protection authorities from powerful member states with stringent data protection laws threatened to block personal data flows to other member states with lax or no data protection laws, pressuring the European Commission and other member states to adopt the Directive (which required all member states to adopt comprehensive, strict data protection laws). In other words, by putting EU single market under threat, these actors have successfully pushed through the Directive, causing the EU to pursue upward harmonization by leveling up data privacy standards across Europe. See EU Data Protection Directive, art. 1; Newman, *supra*, at 113-18.

[1305] NEWMAN, *supra*, at 116, 188 (fn.69).

[1306] Group of Negotiations on Services, Multilateral Trade Negotiations – Uruguay Round, Communication from the European Communities, MTN.GNS/W/105, Article XV(c) (18 June 1990) (providing that "the parties may adopt or enforce measure necessary to protect personal data and individual privacy subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between parties where like conditions prevail, or a disguised restriction on international trade in services").

[1307] Chander and Schwartz, *supra*, at 15 (noting that "[w]hen the United States tabled its proposed text for the new agreement for trade in services in October 1989, privacy was nowhere to be found," and that after the EU's proposal as such, "Japan's proposal the following month echoed this approach").

[1308] NEWMAN, *supra*, at 188 fn.69 (citing a 2003 interview in Brussels with a European Commission official responsible for the Directive).

[1309] *Id.*, at 117.

[1310] *Id.*, at 188 fn. 70.

[1311] *Id.* Chander and Schwartz, *supra*, at 15 ("The final GATS text on the privacy exception tracked the 1990 proposals from the European Communities and Japan").

[1312] GATS, art. XIV(c)(ii).

[1313] Appellate Body Report, U.S.-Gambling, WT/DS285/AB/R (April 7, 2005), paras. 304-305.

between countries where like conditions prevail, or a disguised restriction on trade in services."[1314] In practice, this condition requires consistency of enforcement of the measures among WTO member states.[1315] Together, these criteria aim to ensure that the privacy exception would not be misused to pursue protectionism or other illegitimate goals. As such, the GATS privacy exemption reserves a degree of regulatory autonomy for a state to adopt and maintain domestic data privacy law, provided that these measures are non-discriminatory and do not unduly interfere with trade (i.e., satisfy the "necessity" condition).

(b) Implications of the GATS Privacy Exception

With the implementation of the EU Data Protection Directive in 1998, the U.S. came to realize the implications of the privacy exception of the GATS.[1316] U.S. firms, concerned that information flows with their European affiliates would be blocked, turned to the U.S. government to limit the extraterritorial application of the Directive.[1317] This led the U.S. to threaten to bring a WTO action to strike down the Directive, arguing that the EU privacy rules hindered international trade in services.[1318] In response, the EU forcefully retorted that its Data Protection Directive was in full compliance with European commitments under GATS.[1319]

Much to the disappointment of the U.S., the WTO dispute settlement procedure provides only a limited scrutiny over the application of the Directive.[1320] To begin with, it is difficult for the U.S. to demonstrate that the Directive violates the GATS most-favored-nation or national treatment provisions, since the EU Directive does not obviously discriminate against the U.S. or U.S. service providers in its application.[1321] Indeed, the Directive, on its face, equally applies to transfers of personal data to all third countries.[1322] So, too, is its application non-discriminatory between EU-owned and -registered firms and their foreign equivalents.[1323]

More importantly, application of this privacy exception would substantially constrain the claims brought by the US. As the vital privacy interests of EU residents are directly at stake (as opposed to individuals outside the EU), the WTO adjudicators, when assessing the necessity requirement, may be wary of conducting a delicate balancing of competing trade and privacy interests, which risks being too politically sensitive and intrusive.[1324] Likewise, when reviewing whether the "adequacy" process under the Directive is consistently applied (i.e., the non-discrimination

---

[1314] GATS, art. XIV.
[1315] ROLF H. WEBER & DOMINIC STAIGER, TRANSATLANTIC DATA PROTECTION IN PRACTICE 58 (2017).
[1316] NEWMAN, *supra*, at 117, 188 (fn.70).
[1317] Id., at 117.
[1318] Kenneth Cukier, *U.S. Under Fire over "Aggressive" Net Tax Stance*, COMM. WK. INT'L (March 2, 1998), 17 (quoting Ira Magaziner (the senior Clinton Administration official responsible for e-commerce issues): "In general, [the U.S. government] don't recognize an extra-territorial attempt to shut down the electronic flow of data between countries…. According to the principles of international trade, I think that's a violation of WTO rules").
[1319] Frits Bolkestein, *Is Europe Ready for the New Economy?*, Speech in Nijenrode, Breukelen at March 27, 2000 (Bolkestein was the head of the Internal Market Directorate).
[1320] For a different view, see Chander and Schwartz, *supra*, at 9-10.
[1321] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 49-50 (2000).
[1322] *Id.*, at 49.
[1323] *Id.*, at 50.
[1324] *Id.*, at 51.

condition), adjudicators also may refrain from making a close comparison of the specific levels of data protection of third countries. As indicated by an analogous case (the U.S. *Shrimp-Turtle* case), WTO panels and appellate body, instead, would rather focus on reviewing the process through which the EU evaluates foreign data privacy protection.[1325] Unlike the U.S. measures found violative of the WTO rules,[1326] the EU Directive is likely to satisfy the enumerated criteria for implementing permissible extra-territorial measures.

First, the Directive requires foreign countries to ensure "adequate" (i.e., "essentially equivalent" levels of) protection only, as opposed to the unnecessarily stringent "essentially the same" policy of the U.S.[1327] Second, the EU has established the Article 29 Working Party (an EU advisory body composed of national data protection authority representatives) to review and report on third countries' data privacy laws affecting EU residents.[1328] Third, the EU has engaged in long-term, detailed negotiations with the U.S. to discuss data privacy safeguards that can adequately protect EU residents, and that U.S. authorities and firms can access EU officials to comment on the Directive and its application.[1329] Fourth, even under a country-wide ban of data flows, the Directive still allows individual firms to adopt alternative contractual mechanisms (SCCs or BCRs) or derogations (e.g., consent) to transfer personal data outside the EU.[1330] Fifth, the procedures for foreign firms to obtain EU national data protection commissioners' authorization to use such firm-level solutions for data transfers are relatively transparent, and subject to administrative or judicial review.[1331]

In addition, the WTO rules could further shield the EU Directive, as they constrain the U.S.' capacity to unilaterally retaliate against the EU for hurting U.S. commercial interests.[1332] As the Directive may be justified under the privacy exemption, the U.S.'s retaliatory actions would constitute a breach of WTO rules, enabling the EU to file a complaint to the WTO's adjudicators.

In short, under the privacy exemption, the capacity of the US to challenge and weaken European data privacy rules through GATS-based adjudication or unilateral trade retaliation is significantly constrained. By closing off the multilateral trade avenue, the EU strengthened the pressure on the U.S. to engage in direct bilateral negotiations with itself to find an institutional solution for transatlantic data flows. Such dynamics were instrumental for the conclusion of the Safe Harbor

---

[1325] *Id.*

[1326] *Id.*, at 52-53 (finding that the U.S. failed to satisfy the conditions for invoking article XX (general exceptions) of the GATT on these procedural grounds: "(i) The United States required all exporting WTO members to adopt 'essentially the same [conservation] policy,' and not merely 'comparable' ones; (ii) The United States failed to take 'into consideration the different conditions which may occur in the territories... of different members'; (iii) The United States did not seriously attempt to reach a multilateral solution; (iv) Under its country-wide ban, the United States prohibited shrimp imports even where vessels caught them using U.S.-prescribed methods; and (v) The U.S. certification process was not transparent or predictable."). See WTO Appellate Body, U.S.—Import Prohibition of Certain Shrimp and Shrimp Products, WT/DS58/AB/R (October 12, 1998), paras. 69-83.

[1327] Shaffer, *supra*, at 53.

[1328] *Id.*

[1329] *Id.* at 53-54.

[1330] *Id*.

[1331] *Id.*, at 54.

[1332] *Id.*, at 54-55.

agreement (a tailored-made instrument to transfer EU personal data to the U.S.), which established a set of EU data privacy standards for participating U.S. firms to comply with.[1333]

(B) The EU's Privacy Exceptions in International Trade Agreements After the GATS

From 2000 to the late 2010s, the rights to personal data protection and privacy were enshrined in EU primary law as fundamental rights, and thus, became "constitutionalized" under the European legal order.[1334] In 2016, the EU adopted the General Data Protection Regulation (GDPR) to replace the EU Data Protection Directive. Through this new, harder law, the EU hoped to update the European data protection framework, ensure fundamental rights of individuals, further harmonize member states' data protection rules, and strengthen Europe's internal market.[1335] With these notable developments after the Directive, EU data protection law continues to exert an important influence on the EU's international trade agreements post-GATS. Though pursuing trade liberalization in its preferential trade agreements (PTAs),[1336] the EU adopts a more cautious approach to cross-border data flows in international trade policymaking, in efforts to defend and safeguard its regulatory autonomy to implement data privacy measures.[1337]

(a) EU-led PTAs Negotiated Before 2018

Among EU PTAs that were negotiated before 2018, none contains binding provisions on free flows of information across national borders. Rather, these trade treaties often include predominantly aspirational provisions in the e-commerce chapters, despite clear trends of broader and deeper trade liberalization.[1338] While the EU-Chile PTA is the first EU trade agreements to include substantial e-commerce provisions, such commitments are mostly limited to soft pledges to promote e-commerce and enhance cooperation on trade in services.[1339] Afterwards, the EU-CARIFORUM Agreement, EU-South Korea PTA, and Comprehensive Economic and Trade Agreement (CETA) adopt more elaborated and binding language in their e-commerce and services provisions—but still, substantive rules on cross-border data flows (even in the model of article 15.8 of the KORUS) are lacking.[1340]

[1333] NEWMAN, *supra*, at 117.
[1334] Charter of Fundamental Rights of the European Union, arts. 7, 8(1), 2000 O.J. C 364/10; Consolidated Version of the Treaty on the Functioning of the European Union, art. 16 (1), 2010 O.J. C 83/47.
[1335] Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INTERNATIONAL DATA PRIVACY LAW 3, 3-4 (2011). European Commission, A Comprehensive Approach on Personal Data Protection in the European Union, COM(2010) 609 final, April 11, 2010, at 2-12 ["COM(2010) 609"].
[1336] Yelter Bollen, Ferdi De Ville & Jan Orbie, *EU Trade Policy: Persistent Liberalisation, Contentious Protectionism*, 38 J. EUR. INTEGRATION 279, 282, 287 (2016).
[1337] Sveltlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV., 416, 492-93 (2020).
[1338] *Id.*, at 492. Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECO. L. 245, 261 (2018).
[1339] Agreement Establishing an Association Between the European Community and its Member States, of the One Part, and the Republic of Chile, of the Other Part, arts. 20, 104, Nov. 11, 2002, 352 O.J.L. 3 (2002) [EU-Chile PTA]. Mira Burri, *The Regulation of Data Flows Through Trade Agreements*, 48 GEORGETOWN J. INT'L L. 407, 425 (2017).
[1340] EU-CARIFORUM Agreement, chapter 6 (Electronic Commerce); EU-South Korea PTA, chapter 7 (Trade in Services and Electronic Commerce); CETA, chapter 16 (Electronic Commerce). Compare with KORUS, art. 15.8 ("the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across border").

Likewise, in the EU-Japan PTA and EU-Mexico PTA, the EU has expressly refrained from incorporating a free data flows provision in their digital trade chapters.[1341] Instead, these two treaties contain a review clause only, allowing the parties to reassess the need for adding provisions on free data flows in three years.[1342] In the EU-Japan PTA, transfers of personal data were eventually addressed through a mutual adequacy decision granted by both parties to each other a week before that trade agreement became effective.[1343] As noted by Susan A. Aaronson and Patrick Leblond, such an ambivalent position of the EU reflects the divergent stances of the trade and justice Directorates-General within the Commission on how to regulate cross-border data flows in PTAs, while ensuring adequate protection of personal data.[1344] As a result, the Commission did not find common ground on the proper binding language at the time.[1345] On the other hand, the EU incorporated the GATS privacy exemption in these trade agreements.[1346]

Not surprisingly, the EU's approach to cross-border data flows conflicts with the U.S.'s preferred model of PTA provisions, impeding the conclusion of multilateral and mega-regional trade deals governing this issue-area. When negotiating the Trade in Services Agreement (TiSA) at the WTO, the tension between these two approaches to cross-border data flows became a major contentious point, if not a deal breaker, despite the general agreements of participating countries to reduce barriers in service sectors. While the U.S. strongly preferred enforceable commitments to freely transfer information (including personal data) for commercial data processing by default,[1347] the EU was deeply concerned that this approach may undercut European personal data protection, and restrict its regulatory space to protect individuals' data privacy as fundamental rights.[1348]

Likewise, in the Transatlantic Trade and Investment Partnership (TTIP) negotiations, contrary to the U.S. proposal, the EU refused to include any hard law commitments that might undermine its regulatory approach to data protection, despite its general willingness to negotiate provisions on cross-border data flows.[1349] Negotiations of both agreements have been halted, without making substantial progress.

[1341] EU-Japan Economic Partnership Agreement, art. 8.81, July 2018 [EU-Japan PTA]; Modernisation of the Trade Part of the EU-Mexico Global Agreement, chapter 16 (Digital Trade), April, 2018 [EU-Mexico PTA], https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/149d91f8-d2bc-4fca-8a0d-f7b583af2b87/details. See Yakovleva, *supra*, at 493.

[1342] EU-Japan PTA, art. 8.81; EU-Mexico PTA, chapter 16 (Digital Trade), art. XX (Review Clause on Data Flows).

[1343] European Commission, *European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows*, PRESS RELEASE IP/19/421 (January 23, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 [Commission' Press Release 19/421].

[1344] Aaronson & Leblond, *supra*, at 261. See Yakovleva, *supra*, at 479-81.

[1345] Aaronson & Leblond, *supra*, at 261.

[1346] EU-Chile PTA, art. 135(1)(e)(ii); EU-CARIFORUM Agreement, art. 224(1)(c)(ii); EU-South Korea PTA, art. 7.50(e)(ii); CETA, art. 28.3(2)(c)(ii); EU-Japan PTA, art. 8.3(2)(c)(ii); EU-Mexico PTA, chapter 34 (General Exceptions), art. XX(4), https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/205e69a9-d3c4-464a-95f8-12376360774f/details.

[1347] See e.g., TPP, art. 14.11.

[1348] 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*, 14 WORLD TRADE REV. 671, 690 (2015).

[1349] *Id.*, at 691.

(b) 2018 EU Model Exceptions

The EU international trade policymaking took a drastic turn in 2018. In January 2018, the EU endorsed a set of horizontal provisions on cross-border data flows and personal data protection (to be incorporated in EU trade and investment agreements), which were published in July 2018.[1350] The enactment of these model exceptions indicates that the Commission eventually found a workable solution for regulating international data transfers in PTAs, reconciling its commercial interests on cross-border data flows with its normative concerns over data privacy protection.[1351]

First, article A contains horizontal commitments for "ensuring cross-border data flows to facilitate trade in the digital economy",[1352] marking a significant progress of trade liberalization from the (sub-)sector-specific commitments under the GATS. To that end, it explicitly prohibits an enumerated list of *de jure* bans or restrictions on cross-border data flows, including the requirement that localizes the storage and processing of data, the mandatory use of local computing facilities or network elements for data processing (as such or as a precondition for cross-border data transfers), and a ban on storing or processing data abroad.[1353]

Second, article B recognizes protection of personal data and privacy as fundamental rights, and acknowledges the importance of high-standard data privacy protection for building trust in the digital economy and for the development of trade.[1354] More importantly, it provides a "self-judging" privacy exception in language that closely resembles the national security exceptions in the WTO agreements:

> Each Party may adopt and maintain the safeguards *it deems appropriate to ensure the protection of personal data and privacy*, including through the adoption and application of rules for the cross-border transfer of personal data. *Nothing in this agreement shall affect the protection of personal data and privacy* afforded by the Parties' respective safeguards.[1355]

Third, to remove possible uncertainties, two provisions clarify that EU data privacy protection rules and measures are not subject to investor-state treaty arbitrations or regulatory dialogues.[1356]

This set of model clauses has already been incorporated in the EU-UK PTA and the EU-Chile PTA.[1357] The EU has also submitted these provisions in its ongoing trade agreements with New

---

[1350] Recommendation for a Council Decision, COM(2022) 336 final, July 22, 2022, at 1, https://eur-lex.europa.eu/resource.html?uri=cellar:5b2bfd56-01f8-11ed-acce-01aa75ed71a1.0003.02/DOC_1&format=PDF ["COM(2022) 336"]; European Commission, Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements), https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf ["EU Horizontal Provisions"].

[1351] Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" As Transnational Data Governance*, 54 NYU J. INT'L L. POLITICS 1, 37 (2021).

[1352] EU Horizontal Provisions, art. A(1).

[1353] *Id*.

[1354] *Id*., art. B(1).

[1355] *Id*., art. B(2) (emphasis added).

[1356] *Id*., art. B(4); art. X(3).

[1357] COM(2022) 336, *supra*, at 1 (fn.2). See Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland,

Zealand, Australia, Indonesia, India, and Tunisia, and has decided to initiate single-issue trade negotiations with Japan to include them in the EU-Japan PTA.[1358] Moreover, during the current plurilateral negotiations under the aegis of the WTO, the EU has incorporated these provisions in its submission to the Joint Statement Initiative on e-commerce.[1359] By advancing this template at these fora, the EU intends to get its trading partners on board with its own regulatory approach, which protects personal data and privacy as fundamental rights, while promoting cross-border data flows by banning *de jure* data localization measures.[1360]

Collectively, such model clauses indicate that, while both trade and privacy are desirable policy goals to be pursued at the Union level, the EU prioritizes privacy over trade in case of a potential conflict between them. Through the design of default clauses and exceptions on cross-border data flows, EU data privacy law (including its regulation on international transfers of personal data) is shielded absolutely and *a priori*, without being subject to the disciplines of international trade and investment law.[1361]

Compared with the GATS privacy exception, these exceptions are much easier to invoke, since the objective necessity test is replaced by a subjective one and the non-discrimination requirement simply disappears. Evincing the EU's unwavering stance on data protection in international trade policymaking ("protection of personal data is non-negotiable in trade agreements"),[1362] this change reflects the normative high status of data protection and privacy, which have been entrenched in the EU's constitutional framework. Indeed, after the rights to data protection and privacy have been constitutionalized under EU primary law, ensuring high-standard data privacy protection not only concerns the realization and maintenance of an internal market, but is also indispensable for safeguarding fundamental rights and constitutional values of the EU.

Further, the formulation of these model exceptions represents the EU's strategic response to the development and proliferation of U.S.-promoted data transfer clauses in new-generation PTAs.

Framing data transfers primarily as an economic issue, the U.S. has been advancing a trade-based approach to ensure free data flows across national borders by default.[1363] Throughout its PTAs concluded since the 2000s, U.S.-promoted digital trade rules have evolved into stronger protection of free international data flows and stricter scrutiny on national data restrictive regulations,

---

of the other part, art. 201 [EU-UK PTA]. The UK only affirmed that "individuals have a right to the protection of personal data and privacy", without recognizing the fundamental rights status. See id., art. 202. See also EU-Chile Advanced Framework Agreement, December 2022, art. 19.5.

[1358] COM(2022) 336, *supra*, at 1, 3-4; European Union, *EU-Tunisia Free Trade Agreement Proposal on Digital Trade*, November 9, 2018, at 4-5.

[1359] European Union, *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*, WTO Doc. INF/ECOM/22, April 26, 2019, at 4.

[1360] Erie & Streinz, *supra* (*The Beijing Effect*), 38.

[1361] Yakovleva, *supra*, at 495.

[1362] European Commission, *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7 final (January 10, 2017), at 6, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN ["COM(2017) 7"]; Jean-Claude Juncker, *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change—Political Guidelines for the Next European Commission*, October 22, 2014, at 8, https://ec.europa.eu/info/publications/juncker-political-guidelines_en.

[1363] See *supra* chapter 2 ("U.S.-led regime- and forum-shifting"), sections III, IV.

culminating in the TPP and USMCA.[1364] By deploying PTAs to pursue its "digital trade agenda", the U.S. vigorously sought to create the default rules of free data flows across national borders, oblige foreign regulators restricting data transfers (including for data privacy reasons) to justify the legitimacy of such measures as permitted exceptions under the treaty, and promote a permissive set of international minimum data privacy standards (i.e., the APEC CBPR system) to protect international data exchange.[1365] Hailed as "gold standards" for future global digital trade, these provisions have been increasingly emulated in subsequent PTAs concluded by U.S. trading partners and beyond.[1366]

Against such recent notable developments in the international trade regime, these European model exceptions advance a drastically different regulatory approach in PTAs to defend the EU's normative preference. Under this approach, international trade rules cannot challenge domestic regulatory autonomy in pursuit of data privacy protection, which is removed from international adjudication altogether; nor could they use a permissive international privacy floor to water down national data protection levels.

Relatedly, the privacy exception identified above also reveals the influence of the constitutional underpinnings of data privacy protection on the EU's conceptualization of "digital protectionism". While the EU utilizes PTAs as an instrumental tool to set rules for cross-border data flows and to tackle "digital protectionist" practices (just like the U.S.),[1367] it adopts a different conceptualization of "digital protectionism" from that of the U.S.

Following an instrumental approach to data protection in PTAs (i.e., data privacy is protected as an ancillary trade value to facilitate economic flows), the U.S. considers any foreign measures that undercut the efficiency of cross-border data flows as potentially "protectionist", including data protection laws of the EU and its member states.[1368] In contrast, the EU requires its trading partners to accept its data privacy commitments as non-negotiable in trade policymaking, *ex ante* carving out protection of personal data from the realm of "protectionism".[1369]

Though both recognize the importance of data privacy protection, these two conceptions of "digital protectionism" diverge on what they regard as the "correct" level of protection should be, resulting in different baseline positions between data privacy protection and trade protectionism.[1370] In other words, under these different notions of "digital protectionism", the U.S. and the EU come up with different answers on the "right balance" to be struck between the economic interests and societal values (data privacy protection) underlying personal data.[1371]

[1364] Id. See TPP, arts. 14.11, 14.13; USMCA, arts. 19.11, 19.12.
[1365] See *supra* chapter 2 ("U.S.-led regime- and forum-shifting"), section IV.
[1366] Id. See Mira Burri, *Cross-Border Data Flows in Global Trade and Privacy Law*, presented at the 2021 ASIL Mid-Year Research Forum (manuscript on file with the author), at 8 (noting a trend of subsequent PTAs "closely follow the CPTPP template and enhance the diffusion of the rules on data flows and data localization").
[1367] Aaronson & Leblond, *supra*, at 262. See *supra* chapter 2 ("U.S.-led Regime- and Forum-Shifting), section IV.
[1368] Yakovleva, *supra*, at 474-76.
[1369] Aaronson & Leblond, *supra*, at 260, 262. See e.g., COM(2017) 7, *supra*, at 6 (stating that "European companies operating in some third countries are increasingly faced with *protectionist restrictions that cannot be justified with legitimate privacy considerations*") (emphasis added).
[1370] Yakovleva, *supra*, at 481.
[1371] *Id*.

B. Coordinating the EU's "Adequacy" and Trade Negotiations

Traditionally, the EU removes its data protection rules from international trade negotiations, but instead pursues its data protection processes and trade policies on separate tracks.[1372] In particular, the adequacy finding is generally deemed a unilateral decision adopted by the Commission in accordance with EU data protection law and based on its criteria.[1373] Yet, since 2017, the EU increasingly coordinates its data protection and trade policies, using the linkages between data privacy and international trade to strengthen its influence and expand its commercial relations with a third country.[1374] This is exemplified by the EU's simultaneous negotiations of a mutual adequacy decision and a trade agreement with Japan.

After two years' negotiations, the EU and Japan reached a mutual adequacy decision in 2019, allowing personal data to freely flow between these two economies.[1375] Unlike the EU's previous adequacy findings that only covered the flows of European personal data to a third country, this EU-Japan joint decision is reciprocal in nature, recognizing each other's data protection systems as "adequate". For the EU, this adequacy finding of Japan largely rests on the latter's substantial legal reform on data privacy protection. Such initiatives include extensive amendments of Japan's Act on the Protection of Personal Information (APPI) (that moved it substantially closer to the EU system),[1376] Japan's supplementary rules (with the full effects of a legislation) that provide additional safeguards for certain EU-originated personal data (e.g. Europeans' sensitive data),[1377] its special assurance to protect personal data for criminal law and national security purposes,[1378]

[1372] COM(2017) 7, *supra*, at 6, 9 ("Privacy is not a commodity to be traded…. The EU data protection rules cannot be the subject of negotiations in a free trade agreement…. dialogues on data protection and trade negotiations with third countries have to follow separate tracks").
[1373] *Id*., at 9 (fn.42).
[1374] Chander and Schwartz, *supra*, 29, 31.
[1375] Commission' Press Release 19/421, *supra*. Such negotiations began in January, 2017, see European Commission, *Commission Proposes High Level of Privacy Rules for All Electronic Communications and Updates Data Protection Rules for EU Institutions*, PRESS RELEASE IP/17/16 (January 10, 2017), https://ec.europa.eu/commission/presscorner/detail/en/IP_17_16.
[1376] Schwartz, *supra* (The EU Way), at 788 ("These include an expanded definition of sensitive data, greater individual rights, stronger limits on the use of personal data provided to third parties, and enhanced enforcement powers for the Japanese data protection authority").
[1377] Commission Implementing Decision (EU) 2019/49 of 23 January 2019, pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by Japan Under the Act on the Protection of Personal Information, 2019 O.J. (L 76), paras. 30-31; Annex I, at 38, 39, 43 ["Commission Implementing Decision (EU) 2019/49"]; Commission' Press Release 19/421, *supra* (stating that the supplementary rules provide additional safeguards that would strengthen the protection of Europeans' sensitive personal data, the exercise of individual rights, and the protection of onward transfers of EU data to a third country, and will be binding on Japanese firms importing EU data and enforceable by Japanese DPA and courts). Schwartz, *supra* (The EU Way), at 788-90 (noting that some of the supplementary rules, such as the protection for sensitive data, are limited only to EU data; in contrast, the APPI's protection for sensitive data exists, but its definition of sensitive data is narrower and different than the GDPR's approach).
[1378] Commission Implementing Decision (EU) 2019/49, Annex II, at 56 (the applicable limitations ensures that the collection and processing of data for criminal law and national security purposes occur "only to the extent necessary to the performance of specific duties of the competent public authority as well as on the basis of specific threats", excluding "mass and indiscriminate collection or access to personal information for national security reasons"). The Annex II also provides independent oversight and effective redress mechanisms for such use of personal data, see *id.*, at 56-58.

and a dispute settlement mechanism to investigate and resolve Europeans' complaints on access to their data by Japanese public authorities.[1379] In addition, the EU would implement future periodic reviews to scrutinize the validity of Japan's adequacy status, and thus could require improvements on the application and enforcement of these rules.[1380]

Aside from bridging important differences between these two data protection systems, the mutual adequacy decision causes Japan to converge on the EU's data protection model, serving as an entry point for the diffusion of European data privacy policy.[1381] Under the revised APPI, Japan also follows the EU's "adequacy" standard: in principle, it disallows international transfers of personal data to countries without adequate level of data protection.[1382]

In parallel to the reciprocal adequacy negotiations, the EU and Japan have also negotiated a new-generation PTA, the EU-Japan Economic Partnership Agreement.[1383] As the biggest trade deal ever negotiated by the EU, this agreement would remove a wide range of custom duties and regulatory barriers, creating "an open trade zone covering over 600 million people".[1384] To that end, the EU-Japan privacy negotiations complement and strengthen their trade negotiations in three major ways.

First, when selecting a third country for opening "adequacy" discussions, the EU's economic relationship with it (including the existence of a PTA or ongoing negotiations) is an important factor to consider.[1385] Thus, maintaining privacy and trade negotiations in parallel would enhance the EU's bargaining powers when negotiating a trade agreement. As issue-linkage between privacy and trade policies broadens the spectrum of policy trade-offs and enlarges the room for achieving a consensus, the adequacy negotiations also could facilitate and complement ongoing trade negotiations between the EU and Japan.

Second, the completion of a mutual adequacy decision ensures that personal data could freely transfer between European and Japanese markets in ways aligned with EU data privacy standards, substantially removing regulatory barriers to digital trade between these two economies. As stated by Věra Jourová, the Directorate-General for Justice and Consumers, this mutual adequacy finding would create "the world's largest area of safe transfers of data based on a high level of protection for personal data", enabling EU firms to "benefit from uninhibited flow of data with this key commercial partner" and enjoy "privileged access to the 127 million Japanese consumers."[1386] For

---

[1379] Commission' Press Release 19/421, *supra* ("This new mechanism will be administered and supervised by the Japanese independent data protection authority").
[1380] Commission Implementing Decision (EU) 2019/49, paras. 180-182.
[1381] Schwartz, *supra* (The EU Way), at 790.
[1382] APPI, art. 24 (cross-border flows of personal data to a foreign country is not permitted, unless (i) the data subject gives specific advance consent to the transfer, (ii) the recipient country has a legal system deemed equivalent in its data privacy protection, or (iii) the recipient firm undertakes adequate precautionary measures to protect personal data, as required by Japanese DPA), art. 42 (Japanese DPA is vested with a data embargo power).
[1383] European Commission, *EU and Japan Sign Economic Partnership Agreement*, PRESS RELEASE (July 17, 2018), https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4526.
[1384] *Id.*
[1385] COM(2017) 7, *supra*, at 8.
[1386] European Commission, *The European Union and Japan Agreed to Create the World's Largest Area of Safe Data Flows,* PRESS RELEASE IP/18/4501 (July 17, 2018), https://ec.europa.eu/commission/presscorner/detail/ga/IP_18_4501 (quoting Věra Jourová: "Japan and EU are already

Japan, this economic rationale equally applies. As uninhibited transfers of personal data facilitate commercial flows reliant on data, Japan's adoption of a data protection framework modelled on EU regulation is partly a strategic action, complementing and expanding its growing commercial relations with Europe.[1387]

Third, the EU's strategic linking of trade and privacy policies reveals a new model of reconciling international trade law and data privacy law.[1388] Previously, there were substantial tensions between typical commitments to unhindered data flows of international trade agreements (from the GATS to U.S.-led new-generation PTAs), on the one hand, and the EU's regulatory approach to international data transfers under its data protection law (characterized by restrictions or bans on data flows based on the adequacy assessments), on the other hand.[1389] To reconcile such normative tensions and potential conflicts, the EU's simultaneous negotiations of a mutual adequacy decision and an ambitious trade deal with Japan provides a new paradigm that re-orders the "trade-privacy" relationship. Through improved institutional coordination, this model may achieve greater harmony between the data privacy and international trade regimes, while avoiding the subordination of data privacy protection to trade liberalization.[1390] By causing Japan to align its data protection law with European standards, this model seeks to ensure that high-standard data privacy protection and trade facilitation and liberalization go hand in hand in a mutually beneficial manner.[1391]

II. IMPLICATIONS FOR GLOBAL DATA PRIVACY PROTECTION: EU DATA PROTECTION LAW RISING AS THE GLOBAL STANDARDS

In the realm of data privacy protection, the EU has gradually emerged as a global rule-maker. In fact, there are few legal instruments that influenced international digital companies, foreign governments, and consumers alike more than European data privacy regime. Since the mid-1990s, EU data protection rules have become the *de facto* international standards for an increasing number of companies and countries around the world.[1392] Such momentum recently has been accelerated and amplified by the enactment of the General Data Protection Regulation (GDPR), which is "widely regarded as a privacy law not just for the EU, but for the world."[1393]

When this new EU legislation came into effect in May 2018, Internet users worldwide were flooded with a flurry of emails and alerts from numerous companies informing them of relevant privacy policy updates aligned with this regulation.[1394] Heralded as the world's strongest data protection law, the GDPR has caused businesses around the globe to adjust their data collection, storage, usage,

---

strategic partners. Data is the fuel of global economy and this agreement will allow for data to travel safely between use to the benefit of both our citizens and our economies") ["Press Release IP/18/4501"].

[1387] Schwartz, *supra* (the EU Way), at 791; *id.*

[1388] Schwartz, *supra* (the EU Way), at 791.

[1389] *Id.*; Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6. HARV. J. L. & TECH. 287, 295 (1993).

[1390] Schwartz, *supra* (the EU Way), at 792.

[1391] See Commission, *supra* (Press Release IP/18/4501).

[1392] NEWMAN, *supra*, at 36-9; Braford, *supra* (Brussels Effect), at 22-4.

[1393] Schwartz, *supra* (The EU Way), at 771.

[1394] Brian X. Chen, *Getting a Flood of G.D.P.R.-Related Privacy Policy Updates? Read Them*, NEW YORK TIMES (May 23, 2018), https://www.nytimes.com/2018/05/23/technology/personaltech/what-you-should-look-for-europe-data-law.html.

sharing, and transferring practices according to European standards.[1395] National legislators and regulators across different continents, too, have been scrambling to update their domestic data protection laws based on EU standards.[1396]

These aspects raise important questions: why do these foreign companies and governments follow the EU's data privacy rules, even where no Europeans' data are involved? How do European data privacy norms rise to dominate the international market, making the EU such an influential global data privacy regulator in its own right?

This Part delves into this notable phenomenon of policy diffusion. Section A briefly reviews the political economy behind the EU's export of its data privacy norms. Section B discusses multinational companies' adoption of EU data protection standards for their international business conduct. Section C explores the spread of EU data protection rules to third countries, which increasingly converge on the EU regulatory model.

A. The Political Economy Undergirding the EU's Global Rule-Making

While the origin of EU data protection regulation is largely attributed to an inward-looking goal of establishing the European single market, its implementation has generated an ancillary effect of establishing the EU as a "global regulatory hegemon", influencing market participants and foreign governments worldwide.[1397] After realizing such extraterritorial effects of EU rules, the Commission welcomes its newfound external regulatory powers, increasingly underscoring the need to externalize such rules beyond its single market.[1398] Noting that it is emerging as a global rule-maker through internal market regulation, the Commission becomes more active and assertive in using its data privacy rules to shape the global regulatory environment, in pursuit of greater international influence.[1399] For the EU, the importance of this external motive can be explained by the following economic, political, and strategic interests.

From an economic perspective, the externalization of EU data privacy rules as international standards could level the playing field for European companies, preserve the competitiveness of the European industries,[1400] and promote cross-border data flows essential for free trade. Since high-standard data privacy rules typically impose higher compliance costs and administrative

---

[1395] *Id.*

[1396] Mark Scott and Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (May 17, 2019), https://perma.cc/PKM3-BA3V.

[1397] BRAFORD, *supra*, at 7, 21.

[1398] *Id*. (noting that since 2007, the Commission became more self-conscious of the necessity of exporting EU rules abroad and its increased ability to do so across a broad spectrum of market regulation areas).

[1399] See e.g., COM(2017) 7, *supra*, at 11 ("The EU data protection legal framework has often served as a reference for third countries developing legislation in this field. The EU will continue to engage actively in dialogue with its international partners, at both bilateral and multilateral level, to foster convergence by developing high and interoperable personal data protection standards globally"); COM(2010) 609, *supra*, at 16 (arguing that the EU "must…. remain a driving force behind the development and promotion of international legal and technical standards for the protection of personal data, based on the relevant EU and other European instruments on data protection"), 19; Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council: An Area of Freedom, Security and Justice Serving the Citizen*, COM(2009) 262 final (June 10, 2009), at 9, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:en:PDF [" COM(2009) 262"].

[1400] BRAFORD, *supra*, at 23.

burdens on companies, exporting such standards overseas helps to level the playing field for European businesses. If foreign firms adhere to European data protection rules in their home markets, European companies then would be less disadvantaged when competing with them abroad.[1401] To the extent that third countries choose to implement such rules in their domestic legal systems, European firms can operate in these markets based on their home market rules, minimizing the adjustment costs there.[1402] In short, the globalization of EU regulatory standards enables the EU to achieve its social preferences at a lower economic cost, meanwhile preserving the competitiveness of its domestic industries.[1403] Further, by exporting EU-style high-standard data protection globally, the EU hopes to reduce regulatory barriers to cross-border personal data flows across different countries, prospering commerce flows with its trading partners.[1404]

In addition, widespread adoption of EU data protection rules by foreign firms and governments worldwide boosts the legitimacy of EU rules, validating Brussels' regulatory agenda—both at home and abroad.[1405] In this way, the EU's trading partners and foreign investors are less likely to challenge the legality of EU data protection regulation before the WTO, international tribunals under PTAs, or investor-state treaty tribunals alike.[1406] Also, this means that more governments and companies may look to the EU's regulatory rulebook for guidance when searching for international standards (for digital governance or beyond), augmenting the EU's credibility and reputation for setting regulatory benchmarks for the rest of the world.

Furthermore, becoming a global standard-setter for data privacy regulation consolidates the EU's international influence and soft power, boosting its capacity to shape international market regulation and global governance.[1407] When faced with pervasive surveillance by foreign corporate giants and governmental intelligence operations, advancing a rights-based approach to data protection regulation worldwide allows the EU to act as the international guardian of civil liberties and human rights.[1408] This enhances the EU's international status as a benevolent regulatory hegemon and a normative power, enabling it to advance a set of social-welfare-oriented regulatory standards and universal norms globally.[1409] In the global regulatory arena where major great powers' competition over the governing rules for transnational digital governance becomes intensified, the rising dominance of EU data privacy norms empowers the EU to promote a regulatory model that reflects its values and advances its visions and interests, shaping transnational legal order based on Brussels' preferences.[1410]

[1401] *Id.* See e.g., COM(2017) 7, *supra*, at 3 (noting that "the GDPR creates a level playing field between EU and foreign companies in that companies based outside the EU will have to apply the same rules as European companies if they are offering goods and services or monitoring the behaviour of individuals in the EU").
[1402] BRAFORD, *supra*, at 23.
[1403] *Id.*
[1404] COM(2017) 7, *supra*, at 11, 16.
[1405] BRAFORD, *supra*, at 23. DAVID VOGEL, THE POLITICS OF PRECAUTION 13 (2005).
[1406] BRAFORD, *supra*, at 23.
[1407] *Id*., at 23-4. See Ian Manners, *Normative Power Europe: A Contradiction in Terms?*, 40 J. OF COMMON MARKET STUDIES 235, 239, 240-1, 244 (2002).
[1408] BRAFORD, *supra*, at 24.
[1409] Braford, *supra*, at 37-8.
[1410] See Anu Braford & Eric Posner, *Universal Exceptionalism in International Law*, 52 HARV. INT'L L. J. 1, 5 (2011).

B. De Facto *Brussels Effect Among Multinationals*

When implementing European data protection law to regulate its own market, the EU wields unilateral powers to regulate the global marketplace, resulting in *de facto* externalization of EU regulatory standards among foreign companies.[1411] Driven by their commercial interests, international companies respond to EU data protection regulation by adjusting their global business practices and privacy policies to conform with EU rules, extending the EU standards to govern their production and operations worldwide.[1412] Such dynamics convert European data privacy norms into a prominent set of global standards, demonstrating a process of unilateral regulatory globalization (termed as the "*de facto* Brussels effect").[1413]

Indeed, numerous multinational companies choose to adopt EU data privacy standards as their company policies worldwide. In January 2018, Facebook announced that it will make major privacy changes to comply with the GDPR, and would extend European data privacy protection to its 2.2 billion users across the world.[1414] Highlighting strong commitments to ensure GDPR-compliant, Mark Zuckerburg stated that Facebook will "make all controls and settings the same everywhere, not just in Europe."[1415] Apple also adopted a single global privacy policy based on the GDPR, voicing the company's strong belief in data privacy protection as fundamental rights that should not vary based on the geographic location of customers.[1416] Tim Cook, the CEO of Apple, adopted the EU's rights-based discourse, stating "privacy is a fundamental human right."[1417] In pursuant to the principle of "privacy by design" (under article 25 of the GDPR), Apple designs and engineers its products and services to be GDPR-consistent by default, minimizing the collection of personal data through product design from the outset.[1418]

Likewise, Google announced its commitments to ensuring GDPR compliance across its services, and undertook to make important updates and improvements to its privacy policy to directly

---

[1411] BRAFORD, *supra*, at 1.
[1412] *Id.*, at 2.
[1413] *Id.*
[1414] Natasha Lomas, *Facebook to Roll Out Global Privacy Settings Hub—Thanks to GDPR*, TECHCRUNCH (January 24, 2018), https://perma.cc/BK5K-A8AD (noting that Facebook COO Sheryl Sandberg said the company would be "rolling out a new privacy center globally that will put the core privacy settings for Facebook in one place and make it much easier for people to manage their data", and that "[l]ast year the company…. Had assembled 'the largest cross functional team' in the history of its family of companies to support [GDPR] compliance").
[1415] Hard Questions Q&A with Mark Zuckerberg, FACEBOOK NEWSROOM (April 4, 2018), https://perma.cc/NEP5-9748.
[1416] Apple Customer Privacy Policy, APPLE, https://www.apple.com/legal/privacy/ ("At Apple, we believe strongly in fundamental privacy rights — and that those fundamental rights should not differ depending on where you live in the world").
[1417] Apple UK, *Privacy | WWDC 2021 | Apple*, YOUTUBE (June 15, 2021), https://www.youtube.com/watch?v=vu3_01y4sLk&t=4s; *Apple CEO Tim Cook: "Privacy Is A Fundamental Human Right"*, NPR (October 1, 2015), https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right ["NPR"].
[1418] *Privacy Governance*, APPLE, https://perma.cc/42BC-X6MJ/; *id.* ("We work relentlessly to build (privacy) into everything we make. It's fundamental to how we design and engineer every product and service we put into the world…. And that's meant introducing countless features that give users transparency and choice over how their data is collected, used, and shared").

address GDPR requirements—not just to EU users, but those all around the world.[1419] Brad Smith, the CEO of Google, stated that "privacy is not just a fundamental human right," but "a foundational right," and called privacy "the most essential battle of our time."[1420] On May 25, 2018 (the day when the GDPR became effective), Uber similarly released a revised, GDPR-compliant privacy policy, applying to all its users across different jurisdictions.[1421] A 2016 PWC survey shows that U.S. multinationals generally treat GDPR-compliance as a high priority, and are willing to spend more than USD1 million to meet that end.[1422] To date, many multinational firms (including Google, Microsoft, and Netflix) maintain only one corporate-wide privacy policy, which is that of the EU.[1423]

That these firms choose to adhere to EU data protection law (even for their non-EU consumers) should not be surprising. In case of data protection regulation, all the conditions for the *de facto* Brussels Effect (as theorized by Anu Braford) are satisfied, enabling the EU to externalize its regulatory standards by unilaterally regulating its internal market.[1424] First, the EU is one of the world's largest consumer markets, with a relatively high proportion of affluent consumers.[1425] Given the importance of Europe for many data-driven firms, it is not commercially viable for multinational companies to abandon the EU market altogether.[1426] The remarkably high value of market access to Europe makes foreign firms willing to incur even significant adjustment costs to keep trading in the EU.[1427]

Second, the EU has strong regulatory capacity to effectively implement and enforce its data protection regulation on firms subject to its jurisdiction.[1428] With substantial regulatory expertise, powers, and resources at hand, EU regulators could bring regulatory actions to protect EU citizens' data privacy, and may impose hefty sanctions on individual violators to remedy and deter non-

---

[1419] Improvements to Our Privacy Policy and Privacy Controls, GOOGLE (May 12, 2018), https://groups.google.com/g/livesense-dev/c/sR0HJ529Gf8?pli=1 ("We're making these updates as the General Data Protection Regulation (GDPR) takes effect across the European Union.... and we're taking the opportunity to make improvements for Google users around the world"); Suzanne Frey and Marc Crandall, *Google Cloud: Our Commitment to the General Data Protection Regulation (GDPR)*, GOOGLE CLOUD (May 3, 2017), https://blog.google/products/google-cloud/google-cloud-our-commitment-general-data-protection-regulation-gdpr/.

[1420] Neil Hodge, *Microsoft President: Tech Companies Must Embrace Privacy Regs*, Compliance Week (October 24, 2019), https://www.complianceweek.com/data-privacy/microsoft-president-tech-companies-must-embrace-privacy-regs/27937.article (noting that Brad said with that right comes a need for EU style data protection rules); Forrester, *Why Privacy Is "The Most Essential Battle of Our Time"*, FORBES (May 11, 2022), https://www.forbes.com/sites/forrester/2022/05/11/why-privacy-is-the-most-essential-battle-of-our-time/?sh=63a1705c13ff.

[1421] *Privacy Policy*, UBER (May 25, 2018), https://perma.cc/43JZ-MP4N.

[1422] PricewaterhouseCoopers, GDPR Preparedness Pulse Survey (2016), https://perma.cc/2BZB-FGWK (finding that among more than 200 respondents from U.S. firms with more than 500 employees, "54% reported GDPR readiness is the highest priority on their data-privacy and security agenda"; that "[a]nother 38% said GDPR is one of several priorities, while only 7% said it isn't a top priority"; and that "77% plan to spend $1 million or more on GDPR").

[1423] BRAFORD, *supra*, at 143. See *Privacy Policy & Terms*, GOOGLE (January 22, 2019), https://perma.cc/PHQ9-RBDJ; *Privacy Statement*, NETFLIX (April 24, 2019) https://perma.cc/TF7G-H774.

[1424] See BRAFORD, *supra*, at 25 (identifying "market size, regulatory capacity, stringent standards, inelastic targets, and non-divisibility" as the conditions for unilateral regulatory globalization).

[1425] Braford, *supra*, at 12.

[1426] *Id.*

[1427] *Id.*, at 12.

[1428] *Id.*, at 12-4. "Regulatory capacity" refers to the ability of internal regulatory institutions to formulate, monitor, and enforce market rules effectively. See *id.*, at 10.

compliance.[1429] Third, the EU data protection law is characterized by stringent data privacy rules and demanding regulatory standards.[1430] Fourth, the EU data privacy regime primarily regulates consumer markets, whose inelastic, immobile nature makes it difficult for companies to circumvent its regulatory rules by moving to another jurisdiction.[1431] In particular, the GDPR protects EU data subjects targeted by non-EU firms whose processing occurs outside the EU, further expanding its extraterritoriality and making such standards highly inelastic.[1432]

Fifth, for multinational firms, it may not be technically feasible or economically viable to maintain different data protection practices in different markets.[1433] At times, it may be too costly to maintain separate data processing practices or to create special websites just for EU consumers; other times, it is technologically difficult, if not impossible, to separate the data of EU citizens and non-EU citizens.[1434] For instance, the GDPR requires companies to implement principles of "privacy by design" and "privacy by default".[1435] These principles oblige companies to design their products and services with built-in features that conform with EU data protection requirements by default, embedding GDPR standards into the design of the processing systems.[1436] For digital products (such as smartphones, cloud services, and domestic robots), incorporating EU data privacy requirements at the manufacturing or product design stage often makes a company's production or business practice non-divisible across different markets, providing a powerful means to export EU standards across the globe.[1437]

Further, by applying the most stringent regulatory standards to their products and conduct worldwide, digital firms can streamline their global data management systems and internal corporate processes, reducing their overall compliance costs under divergent national privacy regulations.[1438] Due to economies of scale, adopting a single set of global standards (even on more stringent terms) is less costly than conforming to multiple, inconsistent regulatory standards, including laxer ones. For reputational and publicity reasons, multinational companies may also find it difficult to grant high-standard data protection for some consumers only, while denying it for others in a different jurisdiction.[1439] Such a selective practice may incite consumers' boycott and undermine the brand's market value, translating into adverse commercial risks faced by multinational companies. Driven by a combination of these factors (including non-divisibility, economic considerations, reputational and publicity reasons), many multinationals can find it more

[1429] *Id.* It is worth noting that the material resources of powerful multinational firms may outweigh the modest budgets of national DPAs. However, the vast number of regulatory actions completed and underway across various member states show that DPAs are not waiting for their governments to shore up their budgets, while forgoing enforcement of EU data protection law. And multinationals are adopting extensive measures to ensure GDPR-compliance, in anticipation that the EU regulation would be vigorously enforced to police data privacy standards. See BRAFORD, *supra*, at 142.
[1430] BRAFORD, *supra*, at 142.
[1431] Braford, *supra*, at 16-7.
[1432] BRAFORD, *supra*, at 142. See *supra* chapter ("EU's Forum-Shifting"), section III.B.(B)(a).
[1433] BRAFORD, *supra*, at 142-3.
[1434] *Id.*, at 143.
[1435] GDPR, art. 25.
[1436] BRAFORD, *supra*, at 144.
[1437] *Id.*
[1438] *Id.*, at 143-4.
[1439] *Id.*, at 144-5.

beneficial to adopt EU data privacy standards than to customize their practices for different markets.[1440]

As a result, these elements incentivize firms to comply with EU regulatory standards, converting European data privacy rules into dominant global standards ("*de facto* regulatory convergence").[1441] Among these conditions, it is worth noting that a large market alone cannot guarantee *de facto* globalization of regulatory standards. Rather, European data protection law (regulating inelastic targets with stringent and non-divisible standards) and the EU's sufficient regulatory capacity are indispensable mechanisms to translate its market size into a dominant international regulatory influence. Importantly, the creation and development of the EU data privacy regime enable the EU to leverage its market powers to project its regulatory preferences on multinational firms, externalizing its regulatory agenda around the world.

C. The Spread of EU Data Privacy Law among Third Countries

In addition to multinational businesses, foreign governments have also been adopting EU data protection standards. Increasingly, legislatures and regulators in third countries have enacted their own data privacy laws modelled on EU regulation. The following sections firstly provides a brief overview of this phenomenon, and then proceeds to analyze the mechanisms and factors contributing to the global diffusion of the EU model.

(A) The Dominance of EU Data Protection Law as a Globalized Regulatory Model

Since the 1990s, the EU data privacy regime has been highly influential across the globe, generating a remarkable diffusion of the EU model among other countries.[1442] By March 2022, 157 countries have adopted data privacy laws, with most of them following "European standard" data privacy laws.[1443] As the EU data protection law has become the *de facto* international regulatory model, follower countries have changed their domestic laws and policies, expanding data protection regulations in the public and private sectors to align with EU standards.[1444] These countries include large economies and regional economic hubs (such as UK, Japan, South Korea, Australia, Brazil, and South Africa), midsize economies (such as Argentina, Uruguay, Colombia, and Thailand), as well as small economies and island nations (such as Barbados and Bermuda).[1445]

[1440] Paul Schwartz, *The Data Privacy Law of Brexit: Theories of Preference Change*, 22 THEORETICAL INQUIRIES IN LAW 111, 141 (2021).
[1441] Braford, *supra*, 6.
[1442] Schwartz & Peifer, *supra*, at 122; NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 99.
[1443] Graham Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/2022 (March 15, 2022)*, 176 Privacy Laws & Business International Reports 1, 1-9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4137418 (noting that by mid-March 2022, a total of 157 countries have enacted national data privacy law, and "most of these laws are influenced substantially by the EU's GDPR"; that "the EU GDPR (incorporating its predecessor, the 1995 DPD) is clearly the *global template* on which most other countries new laws are based…. ") ["157 Countries"]; GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES 57 (2014) (noting that "something reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws"); Schwartz and Peifer, *supra*, at 122 (noting that "most of the rest of the world follows" EU data protection law).
[1444] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 36, 99.
[1445] BRAFORD, *supra* (BRUSSELS EFFECT), at 148.

But such a notable phenomenon of policy diffusion did not occur overnight. In fact, this trend did not gain momentum until the early 1990s. During the 1970s and 1980s, while advanced western European countries (such as Sweden, Germany, France, the UK) adopted comprehensive data protection laws with stringent standards, this regulatory model motivated little international response from other countries to follow suit.[1446] Rather, after the enactment of the U.S. Privacy Act in 1974, several other largest economies (including Japan, Canada, and Australia) adopted national data privacy laws modelled on this regulatory approach in the 1980s, applying enforceable data privacy principles primarily to the public sector.[1447] Under this U.S. model, data privacy protection of the private sector is largely relegated to business self-regulation and market solutions, with some legislation for select sensitive sectors.[1448] In 1990, only 13 countries enacted EU-style data protection law, among which Israel was the only non- European country. [1449]

When the EU adopted its Data Protection Directive in 1995, the spread of the EU data privacy regime substantially sped up and took a notable upward turn.[1450] From 1990 to 2006, more than 30 countries from 5 continents (including most OECD countries) have enacted comprehensive data protection laws, which govern the processing of personal data in both public and private sectors and establish clear oversight and enforcement mechanisms.[1451] Meanwhile, a number of countries that previously followed the U.S. model have reformed their data privacy laws to adopt comprehensive private sector legislation, moving closer towards EU data protection law. These countries include "Australia, Canada, the Czech Republic, Japan, Lithuania, New Zealand, Slovakia, and Switzerland."[1452]

To be clear, the increasing proliferation of EU data protection law does not mean a lack of institutional competition to regulate data privacy. At the international level, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework seeks to provide an institutional alternative to EU data protection law.[1453] With "a mild prescriptive bite", the framework formulates a set of data privacy standards generally lower than those found in European law, and contains many broad exceptions. [1454] Since the end of 2019, the U.S. has been seeking to promote the APEC Framework's Cross-Border Privacy Rules (CBPR) system to regulate international data transfers, which essentially allows participatory companies and countries to self-certify compliance with these standards. [1455] Treated as having provided sufficient data privacy protection, certified companies are entitled to transfer personal data to overseas certified recipients, without the need

[1446] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 102. *Id.*, at 34 (noting that though "Europe was the locus of comprehensive protection, in 1985 fewer than half of the twelve members of the European Community had any privacy legislation").
[1447] *Id.* For a detailed discussion of the U.S. limited data privacy regime, see *id*., at 23-5.
[1448] *Id.*
[1449] *Id.*, at 36, 102.
[1450] *Id.*, at 102.
[1451] *Id.*, at 36, 103. Braford, *supra*, at 23.
[1452] NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 36-7, 103.
[1453] *Id.*, at 37, 103.
[1454] BYGRAVE, *supra*, at 76.
[1455] APEC, *APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines* (APEC CBPR), November 2019, at 5-10, https://www.privacy.gov.ph/wp-content/uploads/2021/10/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019-1.pdf.

to satisfy additional requirements.[1456] As such, the CBPR system seems to be a weaker version of the Safe Harbor agreement. However, neither the APEC framework nor the CBPR has attracted many countries to participate, and their momentum pales compared with that of EU data protection law.[1457]

As of today, most of national data privacy laws follow the EU model.[1458] Notably, one of the most-often-adopted "European" principles outside the EU is the "adequacy" requirements, conditioning exports of personal data on whether the level of data protection in a third country is sufficient.[1459] Admittedly, this does not mean that these countries have implemented identical national laws in this regard, as specific national data privacy requirements (such as the age for consent, the determination of the "adequacy") and enforcement and implementation mechanisms may vary across different jurisdictions.[1460] Nevertheless, consumers across the world increasingly enjoy enforceable rights of data protection based on European standards for their data collected and processed in the private and public sectors.[1461] In contrast, U.S.-style data privacy law becomes a notable exception at the margin, which has been increasingly "squeezed out as a viable regulatory model in the international political economy."[1462]

(B) Mechanisms and Factors Driving Third Countries' Legal Transplants Worldwide

While the *de facto* Brussels effect largely explains multinational companies' adherence with European data protection standards in their international business practices, the reasons for third countries' emulation of the EU model are more complicated and nuanced.

First, by enlisting multinationals to advocate for the local adoption of EU rules, the *de facto* Brussels effect can change the political economy in foreign jurisdictions, paving the way for the *de jure* Brussels effect to take place.[1463] Second, the adequacy requirements of the EU data protection regulation enable the EU to translate its market powers into a potent negotiating leverage, demanding foreign countries' regulatory adjustment to ratchet up data privacy protection and converge on EU standards.

Third, the EU implicitly or explicitly ties regulatory harmonization to external economic and political advantages, deploying "issue-linkage" politics to incentivize and pressure third countries to adopt EU-style comprehensive data protection law. Fourth, separate from the EU's market

---

[1456] Infocomm Media Development Authority, *APEC Cross Border Privacy Rules (CBPR) System*, October 30, 2019, https://www.imda.gov.sg/programme-listing/Cross-Border-Privacy-Rules-Certification

[1457] See NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 103 (noting that the APEC Privacy Framework "remained essentially a policy document with little implication for cross-border regulation"). See also Graham Greenleaf (@grahamgreenleaf), Twitter (April 22, 2022, 8:58 AM), https://twitter.com/grahamgreenleaf/status/1517306911506706432 (noting that the APEC CBPR lacks momentum, as it has "only 3 active economies with certified companies" after a decade ("USA (36); Japan (3); Singapore (4)"), and that "Canada, Korea, the Philippines & Taiwan just pretend involvement").

[1458] Greenleaf, *supra* (157 Countries), at 1-9.

[1459] GREENLEAF, *supra* (ASIAN DATA PRIVACY LAWS), 57; Chander & Schwartz, *supra*, at 19 (noting at least 61 non-EU countries adopted this "adequacy" requirement for data exports).

[1460] See NEWMAN, *supra* (PROTECTORS OF PRIVACY), at 104.

[1461] *Id.*

[1462] *Id.*, at 37, 103-4.

[1463] BRAFORD, *supra*, at 78.

powers or negotiating strategies, the accessibility of EU data protection law and its normative appeal in the marketplace of ideas encourage foreign governments to voluntarily emulate the EU model, facilitating the global diffusion of EU data privacy rules.

Though not exhaustive, these mechanisms and factors capture the main reasons for the worldwide diffusion of EU data protection law among foreign governments. Either individually or cumulatively, they empower the EU to expand its regulatory model overseas, shaping international regulatory outcomes on Brussels' preferred terms.

(a) De Jure *Brussels Effect*

In addition to extracting regulatory adjustment of private companies, the Brussels effect could also alter the policy preferences of foreign governments. After adjusting to EU rules, export-oriented multinational firms are incentivized to lobby their domestic governments to incorporate these same standards into national laws, so as to level the playing field against their domestic competitors that do not have to comply with such rules.[1464] Within the domestic political arena, the more such firms have already adopted EU data privacy standards, the lesser the political resistance faced by the governments when transplanting EU rules into domestic legal frameworks. Such corporate lobbying efforts not only directly pressure the governments to pursue regulatory adjustment, but also could mobilize and rally broader support of other political forces sharing the same cause (such as civil societies and human rights activists with similar agendas), altering the political and economic dynamics in domestic policy debates.[1465] As a result, by changing the preferences of dominant domestic business interests, the *de facto* Brussels effect may establish a political economy leading foreign legislators and regulators to affirmatively adopt European regulatory standards, achieving the "*de jure* regulatory convergence" (termed as the "*de jure* Brussels effect").[1466]

A typical example in this regard is the U.S. case. Corporate America has not only adhered to EU data protection regulation, but also vocally advocates for regulatory adjustment by the U.S. government, calling for an EU-style data privacy law to govern the private sector. In October 2018, Apple's chief executive, Cook, publicly articulated the company's "full support" for a comprehensive U.S. federal data privacy law to protect American consumers against private firms.[1467] Cautioning pervasive surveillance of individuals' personal data by state authorities and digital companies alike, Cook stated that "it is time for the rest of the world, including (the U.S.)" to follow the EU's lead to adopt a strict data privacy law.[1468] This stance strongly echoes his previous narrative that Apple believes "privacy is a fundamental human right."[1469]

[1464] *Id*., at 148.
[1465] For instance, the lobbying initiatives of domestic business interest groups for adoption of EU data protection law could bolster similar arguments of privacy advocates and activists, creating a political environment favoring legal reform.
[1466] BRAFORD, *supra*, at 2-3. For a strict definition of the "*de jure* Brussels Effect", see id. (defining it as "the regulatory adjustment that follows from the lobbying efforts by firms that have experienced the de facto Brussels Effect").
[1467] *Tim Took Calls for US Federal Privacy Law to Tackle "Weaponized" Personal Data*, GUARDIAN (October 24, 2018), https://perma.cc/TG55-FTMB ["GUARDIAN"].
[1468] *Id.* ("Our own information, from the everyday to the deeply personal, is being weaponised against us with military efficiency…. This is surveillance, and these stockpiles of personal data only enrich the companies that collect them").
[1469] See *supra* note (NPR).

Even more remarkable are similar policy proposals raised by other U.S. tech giants, whose business models are much more reliant on collecting and commercializing user data than is Apple. For instance, Google proposed a U.S. legislative framework built on the GDPR, extending many of its data privacy principles to global users.[1470] Likewise, Facebook CEO Zuckerberg called for national regulators across different countries to adopt comprehensive data protection regulations consistent with the GDPR, constituting "a common global framework" to protect individuals' personal data against abuses and mishandling.[1471]

The rationale underlying these proposals is similar: given that the GDPR has already governed much of the business practices of these multinationals, enactment of such EU standards in their home market ensures that they would not be disadvantaged when competing domestically against non-EU-exporting firms that need not comply with the Regulation. Further, having a uniform federal data privacy law avoids the problem of complying with a patchwork of potentially inconsistent, or even conflicting, state-by-state data protection laws (including the California Consumer Privacy Act), which may further add to their domestic compliance costs.[1472] While such initiatives have not been successful thus far in the U.S., which remains a notable exception resisting the EU's model of data privacy protection, the U.S might not be able to hold out forever, given the ever-growing momentum pushing for a comprehensive federal data privacy law.[1473] At the very least, acceptance of EU data privacy norms by these most influential data-driven multinationals changes domestic political landscape in ways favoring institutional change, and makes it much easier for the government to *de jure* implement these rules domestically.[1474]

(b) The Potency of the "Adequacy" Requirements

Another powerful policy mechanism at the core of the global diffusion of EU-style data protection law is the EU's regulatory approach to international data transfers. Under this approach, an adequacy finding enables free flows of personal data from the EU to a third country, without the need for data processors to provide contractual safeguards or obtain administrative authorizations from European regulators.[1475] Thus, an adequacy decision provides an privileged access to the European internal market (as if that third country is an EU member state), opening up unimpeded commercial channels for foreign data operators to trade with the EU.[1476] In contrast, for countries without adequate data protection, their companies need to adopt more costly, burdensome, and time-consuming contractual solutions (SCCs and BCRs),[1477] which are subject to additional conditions and face significant legal uncertainty under the *Schrems* decisions.[1478] Meanwhile, EU

[1470] See *supra* note (GUARDIAN).
[1471] Mark Zuckerberg, *The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (March 30, 2019), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.
[1472] BRAFORD, *supra*, at 149. Mehreen Khan & Tim Bradshaw, *Apple and Facebook Call for EU-Style Privacy Laws in US*, FINANCIAL TIMES (October 24, 2018), https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713.
[1473] BRAFORD, *supra*, at 155.
[1474] Schwartz, *supra* (Brexit), at 140-1.
[1475] COM(2017) 7, *supra*, at 4.
[1476] *Id.*
[1477] See *supra* chapter 3 ("EU's Forum-Shifting"), section II.C.(C).
[1478] *Id.*, at section IV.B.

regulators are vested with the authority to block transfers of personal data from the EU market to such countries.[1479] Characterized by a "carrot and stick" approach, the adequacy standard enables the EU to leverage access to its large market to demand third countries' legal reform to improve data privacy protection, translating the EU's market clout into its international regulatory influence. By playing into its trading partners' export dependency and economic reliance on its internal market, the adequacy requirements alter the costs to foreign governments of inaction, pressuring regulators outside the EU to follow European data privacy standards.

While the *de jure* Brussels effect acts *unilaterally* to spread the EU's influence, the adequacy requirements provide the EU with an important bargaining leverage at the negotiating table, enabling it to require institutional change from third countries to converge on EU data privacy standards.[1480] Coupled with the EU's regulatory capacity to monitor the adequacy of other national data privacy regimes, the adequacy requirements bolster the EU's negotiating position to demand sufficient regulatory adjustment.[1481] Indeed, the process leading to an "adequacy" determination usually begins with multiyear discussions and negotiations, during which the Commission may require that third country to revise its data privacy laws to strengthen its level of data protection.[1482] If that third country reforms its data privacy law, the Article 29 Working Party (under the Directive) or the European Data Protection Board (under the GDPR)—mainly composed of national data protection authorities—would evaluate such efforts, and issue an opinion on the adequacy decision, subject to the approval of EU member state representatives and the final adoption by the Commission.[1483] Concerned with the difficulties of commercial data transfers without an adequacy finding, many third countries are strongly incentivized to amend their domestic laws to align with EU standards.[1484] As such, the adequacy requirements regulating European market access, backed by expert EU negotiators and data privacy regulators, enable the EU to press for externalization of its regulatory model across different countries.[1485]

As noted earlier, Japan's case illustrates such dynamics. During its adequacy negotiations with the EU, Japan had substantially amended its APPI in 2015 to bring it in line with the GDPR, which was instrumental for achieving the adequacy status.[1486] Likewise, South Korea followed suit. After starting the adequacy talks with the Commission in January 2017, South Korea reformed its Personal Information Protection Act (PIPA) in 2020 to satisfy the EU's concerns on data privacy protection.[1487] Previously, the PIPA already provided many similar data protection principles, safeguards, individual rights, and corporate obligations as the GDPR, bearing a close resemblance

[1479] EU Data Protection Directive, art. 25; GDPR, art. 44.
[1480] Schwartz, *supra* (The EU Way), at 774. While the underlying dynamics (featuring incentives arising from the attractiveness of market access) of this process are not different from the *de jure* Brussels effect, the regulatory adjustment here is driven by bilateral discussions and negotiations on the adequacy determinations, rather than market-driven unilateralism. See BRAFORD, *supra*, at 78.
[1481] NEWMAN, *supra*, at 110.
[1482] Chander & Schwartz, *supra*, at 18.
[1483] *Id.*; KUNER, *supra*, at 65.
[1484] BRAFORD, *supra*, at 150.
[1485] See NEWMAN, *supra*, at 110.
[1486] See *supra* Section I.B.
[1487] *EU and South Korea Complete Adequacy Talks*, PRIVACY LAWS & BUSINESS (March 30, 2021), https://www.privacylaws.com/news/eu-and-south-korea-complete-adequacy-talks/.

to the EU framework.[1488] However, unlike the EU, South Korea lacked independent enforcement and oversight agencies under its domestic law.[1489] To fill this institutional gap, the amended PIPA established independent data protection authority, vested it with effective powers (including robust sanctioning authority) to implement and enforce data privacy law, and mandated it with similar responsibilities as under the GDPR.[1490] As part of its commitments during the adequacy negotiations, South Korea also provided additional safeguards to level up the protection of EU-originated personal data processed within its border, including greater transparency requirements and stronger protection for onward data transfers (by ensuring the same level of protection for subsequent transfers to third countries).[1491] With its concerns addressed, the Commission rendered an adequacy decision in December 2021.[1492]

For emerging markets, an adequacy decision may bring in the much-needed economic resources to develop the local businesses and technology sectors. Since an adequacy decision enables unrestricted data flows with a third country, European companies are more likely to establish foreign branches or subsidiaries, outsource data-associated operations, or engage local services and businesses (such as call operations or data centers) in that country.[1493]

Uruguay took this view, and considered an adequacy decision as important for attracting European investment and outsourced digital services.[1494] Indeed, Uruguay XXI, the Uruguayan Investment and Export Promotion Agency, stated that the EU's adequacy decision "will open the possibility for major European investments, in particular it will help Uruguay boost its outsourcing industry (call centers, data centers, technology parks) and attract more EU-based companies looking for providers of administrative, financial and other data processing services in Latin America."[1495] Directly driven by the motivation to obtain an adequacy decision, Uruguay adopted its 2008 and 2009 data protection laws, which were closely modelled on the EU Data Protection Directive to converge on EU standards as far as possible.[1496] Such initiatives eventually earned Uruguay an adequacy finding in 2012,[1497] making it the second Latin American country obtaining such a status (after Argentina).[1498]

[1488] *Data Protection: European Commission Launches the Process Towards Adoption of the Adequacy Decision for the Republic of Korea*, PRESS RELEASE (June 16, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2964.
[1489] BRAFORD, *supra*, at 151.
[1490] *Questions & Answers on the Adoption of the Adequacy Decision Ensuring Safe Data Flows Between the EU and the Republic of Korea*, QUESTIONS & ANSWERS (December 17, 2021), https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_6916.
[1491] *Id.* (noting that "these rules are binding and enforceable by (DPAs) and Korean courts").
[1492] *Id.*
[1493] Manuel Martinez-Herrera, *From Habeas Data Action to Omnibus Data Protection: The Latin American Privacy (R)Evolution*, LEXOLOGY (October 5, 2011), https://www.lexology.com/library/detail.aspx?g=5f6d4229-5c79-4513-9b15-18dddd5c6a57.
[1494] BRAFORD, *supra*, at 150.
[1495] Martinez-Herrera, *supra*.
[1496] Arturo J. Carrillo & Matias Jackson, *Following the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, 16 VIENNA J. INT'L CONST. L. (forthcoming 2022), at 58; BRAFORD, *supra*, at 150.
[1497] Commission Implementing Decision, of 21 August 2012 pursuant to Directive 95/46/EC, on the Adequate Protection of Personal Data by the Eastern Republic of Uruguay with Regard to Automated Processing of Personal Data, 2012 O.J.(L227), at 11.
[1498] Carrillo & Jackson, *supra*, at 35.

Further, when launching adequacy discussions, the Commission consciously seeks to create "role models" for other countries in the same region to follow subsequently. Oftentimes, the Commission's selection of countries with which to start the "adequacy" talks is strategic, as it tends to prioritize countries that play a pioneering role in developing national data protection law in their region.[1499] Again, Uruguay is a typical example.[1500] Given that Uruguay was among the few Latin American countries that enacted comprehensive data protection laws based on the EU model, this adequacy decision could spur other neighboring countries (especially those that view Uruguay as a regional competitor) to follow suit, catalyzing the spread of EU data protection regulation across the region.[1501] In other words, the EU's strategic initiation of the adequacy talks or negotiations with a select country could create a competitive environment for neighboring states (that hope to maintain a competitive advantage in the regional markets) to converge to European data protection standards, creating peer pressure to facilitate the norm diffusion process.

To obtain adequacy determinations, numerous countries across Latin America, Africa, and Asia have modelled their national data protection laws on EU regulation, and that number seems to be ever growing.[1502] This is not surprising, since an adequacy decision by the Commission could open unrestricted data transfers and facilitate foreign investment flows with these emerging markets, providing them with valuable opportunities to develop their data-driven and -related sectors.[1503] In Latin America, following the precedents of Argentina and Uruguay, Columbia, Costa Rica, Mexico, Peru, and Brazil have adopted EU-style comprehensive data protection laws, in pursuit of their own adequacy decisions from the Commission.[1504] Likewise, in 2008, Senegal adopted its domestic data protection law, which not only bore a strong resemblance to the EU Data Protection Directive and French data protection law, but also established independent data protection authority to oversee its implementation.[1505] In 2013, South Africa enacted a data privacy law that closely followed the EU Data Protection Directive and contained many key definitions of the GDPR.[1506]

Finally, compared with the EU Data Protection Directive, the GDPR imposes a stronger impetus for third countries to bring their data protection laws in line with EU regulation. On the one hand, the GDPR contains stronger data protection standards, creating urgent needs for other countries to update and adjust their domestic data protection regulations accordingly. On the other hand, the GDPR mandates the Commission to periodically review and closely monitor its adequacy decisions, which must adapt or even withdraw such findings to reflect subsequent development

[1499] COM(2017) 7, *supra*, at 7-8.
[1500] *Id*., at 7.
[1501] For a detailed discussion of the "competition" mechanism for policy diffusion, see *infra* Introduction chapter, section III.C., footnotes 72 to 74 and accompanying text; see also Frank Dobbin, Beth A. Simmons, and Geoffrey Garrett, *The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning*, 33 ANNUAL REVIEW OF SOCIOLOGY 449, 457-58 (2007).
[1502] BRAFORD, *supra*, at 152.
[1503] See Martinez-Herrera, *supra.*
[1504] *Id.*; BRAFORD, *supra*, at 153. For a different view, see Carrillo and Jackson, *supra*, at 72-3 (arguing that Latin American countries' historical ties with EU law, the normative appeal of the EU regulation's rights-based approach, and the GDPR's legal innovations with key data protection concepts are more important than market forces).
[1505] BRAFORD, *supra*, at 152.
[1506] *Id.*, at 152.

affecting the level of protection in a third country.[1507] This expanded power further pressures third countries that already obtained an adequacy decision to conduct necessary legal reforms to maintain their adequacy status. The examples of Argentina and Uruguay suffice to illustrate such dynamics.

Three years after adopting its 2000 data protection law that closely resembled Spain's and EU data protection law, Argentina obtained the EU's adequacy determination.[1508] While that data protection law remained mostly unchanged for over two decades, the GDPR substantially disrupted this legislative status quo. In 2016, Argentina established a working group to study legal reforms necessary to maintain its adequacy status under the GDPR.[1509] Recognizing the gaps and shortcomings of the old framework, Argentina introduced three bills from 2018 to 2020 to reform its data protection law.[1510] Though still pending, these bills incorporated a majority of the GDPR's key elements, and may substantially align Argentina's data protection law with EU rules.[1511] Likewise, in 2018, Uruguay adopted a series of legislative acts to align its data protection system with the GDPR, in efforts to preserve its adequacy standing under this Regulation.[1512] These acts transplanted many of the GDPR's data protection requirements, including the principles of privacy by design and by default, the duty to conduct data protection impact assessment and to designate a DPO, and the data breach notification obligation.[1513] Through these amendments, Uruguay became the first Latin American country that has reformed its data protection law to conform with the GDPR.[1514]

(c) Issue-Linkages

A third mechanism that enables the EU to promote its regulatory model overseas and extract foreign regulatory adjustment is "issue-linkages". By linking adoption of comprehensive data protection law with external economic and political advantages, the EU incentivizes and pressures other countries to align with EU data protection regulation. In this regard, two notable examples exemplify the potency of this mechanism to diffuse EU data protection law.

First, the adequacy requirements *implicitly* link adoption of EU-style data protection law with outbound European investment in the information technology sector, incentivizing developing countries and emerging markets to align their data privacy laws with the EU model. As noted earlier, since an adequacy decision significantly reduces the costs of transferring personal data and operating digital trade with a third country, European companies are incentivized to make investment and outsource digital services in that market. In addition to directly influencing foreign governments, this mechanism can also attract their domestic firms to get on board with EU standards, shaping the preferences of the business interest coalitions in these markets. For instance, Indian firms active in call center operations and software development not only adopted EU data

[1507] See GDPR, art. 45(4)-(6); see also *supra* chapter 3 ("EU's Forum-Shifting"), section III.B.(B).(d).(1).
[1508] BRAFORD, *supra*, at 150.
[1509] *Id.*
[1510] Carrillo & Jackson, *supra*, at 36-7.
[1511] *Id.*, at 37 (noting that the 2018 bill had lapsed during the COVID, but two 2020 bills were still pending).
[1512] *Id.*, at 31.
[1513] *Id.*, at 29, 59-61.
[1514] *Id.*, at 59.

protection standards themselves, but also pressed for domestic legislation modelled on EU regulation to be enacted.[1515]

Second, the EU *explicitly* makes adoption of comprehensive data protection law a condition for obtaining EU membership.[1516] With many potential accession countries highly valuing EU membership for economic and political reasons,[1517] the EU conditions accession to the Union on an applicant's adoption of the EU regulatory playbook, leading to convergence of regulatory standards in line with the EU's expectations.[1518] When reaching accession partnership agreements with potential members, the EU requests these countries to adopt the EU's body of law (*acquis communautaire*), which includes the EU Data Protection Directive or GDPR.[1519] Between 1995 (when the EU Directive was enacted) and 2008, 15 applicant countries adopted comprehensive data protection laws to meet the accession requirements.[1520] When annually reviewing such applicants' progress in fulfilling the preconditions for accession, the EU kept monitoring their domestic data protection levels and pointed to their respective legal and institutional inadequacies, pressing for further reform of their legislative frameworks.[1521] Meanwhile, through a series of assistance programs, the EU provided such candidate countries with legal and technical expertise and financial support, enabling them to build their administrative and institutional capacity necessary for a functioning domestic data protection regime.[1522]

Under such pressures, other countries—which aspired for EU memberships, yet were not applicant countries (including Albania, Bosnia and Herzegovina, and Servia)—have also adopted national data protection laws modeled on the EU Data Protection Directive.[1523] Strikingly, given their relatively immature digital and technological industries, these countries passed such data protection laws far ahead of their domestic economic needs for such rules.[1524]

In short, by conditioning EU accession to regulatory harmonization on data privacy protection, the EU could export its data protection standards to potential EU members, shaping their regulatory reforms on its favorable terms.

(d) Accessibility and Normative Appeal of the EU Model

In addition to these major mechanisms of policy diffusion identified, there are two additional factors that facilitate the widespread emulation of EU data protection law by foreign governments—one pragmatic and one normative. As part of the pulling and pushing forces behind the policy diffusion, these two factors amplify the dominance of the EU's regulatory model as the *de facto* global standards.

[1515] NEWMAN, *supra*, at 165 (fn.43).
[1516] *Id.*, 113.
[1517] *Id*., at 112 (noting that they generally "view membership as an economic and political advantage that will stimulate their economy and integrate them solidly into the fold of western European democracy").
[1518] *Id*., at 112-3.
[1519] *Id*., at 113.
[1520] *Id*.
[1521] *Id*.
[1522] *Id*., at 113-5 (noting such examples include the Czech Republic, Latvia, Lithuania, and Malta).
[1523] *Id*., at 114-5.
[1524] *Id*.

The pragmatic reason is the accessibility of the EU data protection law, making this regulatory model highly transplantable outside the EU.[1525] From the Directive to the GDPR, the EU data protection regulation features a comprehensive legislative framework, applying a common set of data privacy principles and rules to all sectors of the economy and the public sector.[1526] The ease of enactment and comprehensiveness make the EU model a better candidate for legal transplantation, in comparison with the sector-specific and more fragmented U.S. data privacy law (which seems complex and obscure for beginners).[1527] Also, unlike regulations of common law jurisdictions (such as the U.S.), EU data protection law is characterized by more precise and detailed rules.[1528] Such a detailed legislative template, supplemented by data protection authorities' guidelines, interpretations, and recommendations, make these rules easier to emulate and more prone to diffusion, while enhancing their legal certainty and predictability.[1529] For developing countries with inadequate legal and administrative capacity, detailed and codified data protection norms such as these can substitute for a lack of human capital, and thus, are easier to apply, implement, and enforce than more complex, flexible standards.[1530] These attributes makes EU data protection law a relatively simple and straightforward model for third countries to emulate.

Another factor is the normative appeal of EU data protection rules, making them a highly attractive model for emulation.[1531] Representing a rights-based approach ensuring high-standard protection for individuals in a highly interconnected world, EU data protection rules often appeal to foreign legislators, regulators, and policymakers alike,[1532] making them a success in the global marketplace of ideas.[1533] The normative appeal of EU norms can be attributed to the EU's conceptualization of data privacy protection as fundamental rights, anchored in human dignity, personality, and informational self-determination.[1534] This construction seems loftier and more noble than the conceptual framing that regards data privacy largely as a consumer interest in the data marketplace.[1535] Also, such appeal comes from EU regulation's normative innovations—including the right of data portability, the right to be forgotten, the principles of privacy by design and by default—which are widely perceived as the "best formulation" of data protection norms currently available.[1536] In short, such an "ideational influence" of the EU model rests on its normative powers of persuasion and the quality of its ideas.[1537] Independent of the EU's market

[1525] Schwarz, *supra* (The EU Way), at 810-1.
[1526] *Id.*, at 810.
[1527] *Id*., at 812, 818. BRAFORD, *supra*, at 79.
[1528] BRAFORD, *supra*, at 79.
[1529] *Id*.
[1530] *Id*. Hans-Bernand Schafer, *Rules versus Standards in Rich and Poor Countries: Precise Legal Norms as Substitutes for Human Capital in Low-Income Countries*, 14 SUP. CT. ECON. REV. 113 (2006).
[1531] Schwartz, *supra* (The EU Way), at 816.
[1532] Carrillo & Jackson, *supra*, at 72.
[1533] Schwartz, *supra* (The EU Way), at 818. In the global "marketplace of ideas", different policy concepts and regulatory models compete against each other. See *id*., 817.
[1534] Schwartz & Peifer, *supra*, at 123-27.
[1535] *Id*., at 132-37 (comparing the dominant European and U.S. conceptualizations of data privacy). Schwartz, *supra* (The EU Way), at 773 ("the U.S. legal system views information privacy as based largely on a consumer interests. It situates individuals in a data market place in which they are to be free to engage in data exchanges, and the law is to police data trades for unfairness, deceptions, and other market failures").
[1536] Carrillo & Jackson, *supra*, at 72.
[1537] BRAFORD, *supra*, at 81.

powers and negotiating strategies, the normative appeal enables EU data protection rules to set a "virtuous example" for the rest of the world, contributing to their diffusion across different countries.[1538]

III. CONCLUSION

Through two case studies, this chapter systemizes the prominent influence of the EU data privacy regime for the transnational regime complex governing cross-border personal data flows. More than a set of regional data privacy norms, EU data protection law not only shapes the international trade regime in notable ways, but also has been increasingly accepted worldwide as the *de facto* international data privacy standards. In the international regulatory arena where different great powers promote distinct regulatory approaches,[1539] the European data privacy regime enables the EU to make a powerful claim to set the regulatory standards for international personal data transfers.

To begin with, European data protection law has substantially influenced the EU's international trade policymaking. On the one hand, the development of European data protection law led EU negotiators to formulate and reinforce privacy exceptions in international trade agreements, designed to shield EU data privacy rules from being challenged through international adjudication. From the GATS privacy exception to the 2018 EU model exceptions, these provisions have evolved into stronger terms and become easier to invoke. Rather than setting international minimum data privacy standards for cross-border data flows (as is the APEC CBPR system incorporated in the USMCA), the EU simply brackets data protection regulation in its international trade agreements.[1540] Different from the data transfer provisions of U.S.-led new-generation PTAs, these European exemptions safeguard and ensure the exclusive authority of the EU data privacy regime to regulate data privacy protection and cross-border transfers of personal data.

On the other hand, the EU increasingly leverages the issue-linkage of "trade-privacy" to coordinate its "adequacy" and trade negotiations simultaneously. Through parallel negotiations as such, EU data protection law complements and empowers European trade policymaking, enabling the EU to expand its foreign commercial relations, address regulatory barriers hindering digital trade flows, and reconcile trade liberalization with data privacy protection.

Moreover, though originally designed to regulate EU single market, European data privacy norms have been increasingly diffusing around the world and gaining international dominance. Recognizant of the effects of its regulation beyond European market, the EU embraced and leveraged such external regulatory powers to pursue its interests and international influence. From the EU Data Protection Directive to the GDPR, EU data protection law has been increasingly diffusing into multinational companies' business practices and foreign countries' data protection laws, substantially expanding the EU's sphere of regulatory influence worldwide.

In this process, the role of EU data protection law is paramount. First, through the Brussels effect (both *de facto* and *de jure*), EU data privacy rules enable the EU to unilaterally regulate the global

---

[1538] *Id*.
[1539] See *supra* chapter 1 ("A Battle of the Big Three"), section II.A.-C.; Aaronson & Leblond, *supra*, at 268-9.
[1540] Chander & Schwartz, *supra*, at 8.

marketplace, using market mechanisms to transmit EU data protection law to foreign companies and regulators alike. Second, EU data protection norms allow the EU to leverage its market powers to bolster its negotiating leverage, causing third countries to adopt the EU model to regulate data privacy. Third, due to their accessibility and normative appeal, EU data privacy rules provide an easily transplantable and highly attractive regulatory model for foreign governments to emulate, facilitating their global diffusion into other legal systems. In short, European data protection law empowers the EU to leverage and amplify its market powers, negotiating clout, and ideational influence, externalizing its data privacy standards around the globe.

As a regulatory model that reflects the EU's values and serves its interests, European data protection law regulates international personal data transfers based on Brussels' preferences. With a growing dominance of EU data privacy rules, the EU has been increasingly shaping international regulatory outcomes on its own preferred terms, projecting its values, laws, and institutions onto the rest of the world.

Chapter 5

"Data Sovereignty" Unchallenged? The Evolving Domestic Data Governance Regime of China and Its International Implications

Table of Content

INTRODUCTION **228**

I. CHINA'S VISION OF "CYBER SOVEREIGNTY" AND "DATA SOVEREIGNTY": THE NORMATIVE FOUNDATION FOR CHINA'S DOMESTIC DIGITAL GOVERNANCE **231**

A. Regime Security and the Great Firewall ***232***

B. Cyber Sovereignty ***234***

C. Domestic Data Governance in Pursuit of Data Sovereignty ***240***

II. THE POLITICAL ECONOMY UNDERGIRDING CHINA'S DATA LOCALIZATION MEASURES . **247**

A. Protection of National Security Interests ***247***

B. Development of Digital Industry and Technologies ***250***

III. CHINA'S LEGISLATIVE FRAMEWORK GOVERNING DATA SECURITY AND CYBERSECURITY **255**

A. Legislations and Regulations From the 1990s to 2016 ..... ***255***

B. Legislations and Regulations From 2017 to Present ***257***

(A) Cybersecurity Law 257

(B) Personal Information Protection Law 258

(C) Data Security Law 262

IV. REGULATORY INSTITUTIONS **264**

V. IMPLEMENTING REGULATIONS **266**

A. Concretizing Three Mechanisms of Cross-Border Data Transfers ***267***

(A) Security Assessments as the Safety Valve of Cross-Border Data Transfers 267

(B) Alternative Mechanisms of Certification and Standard Contractual Agreements 271

(C) "The Hard Way Out?" 274

B. Sector-Specific Regulations: The Example of the Automobile Sector ***275***

C. Cybersecurity Review over Foreign Listings of Chinese Digital Platforms ***278***

(A) The Domino Effect Generated by Didi's U.S. Listing 279

(B) The Policy Rationale 280

(C) New Rules of Cybersecurity Review 282

D. Draft Network Data Security Management Provisions to Implement the CSL, DSL, and PIPL ***284***

VI. IMPLICATIONS OF CHINA'S REGULATORY APPROACH ON ITS INTERNATIONAL RULEMAKING 287

A. International Trade Negotiations 287

(A) WTO Negotiations 288

(B) Preferential Trade Agreements 290

B. Transnational Data Privacy Rulemaking: The Case of the APEC CBPR System 292

CONCLUSION 295

Introduction

The cyberspace regulation of the People's Republic of China (PRC) often poses distinctive puzzles for an international audience trying to understand its various complexities and nuances. With the largest population of Internet users and a growing number of internationally competitive tech companies, China is the world's second-largest digital economy after the U.S., standing at the forefront of commercializing online business models.[1541] Meanwhile, China has one of the most tightly regulated cyberspaces across all countries, widely known as a practice of "digital authoritarianism".[1542] While cyberspace is often deemed an intangible domain and a primarily unterritorial medium defying geographical borders, China advocates for a concept of "cyber sovereignty", asserting governmental control over its population's access to online information within its territorial boundary.[1543] Likewise, though data transits the globe via cyberspace, China

---

[1541] *China's Digital Economy Hits &7.1T: White Paper*, STATE COUNCIL OF THE PRC (July 30, 2022), http://english.www.gov.cn/archive/statistics/202207/30/content_WS62e515e6c6d02e533532eb06.html ("China's digital economy reached (USD)7.1 trillion in 2021…. ranking second after the United States…. (And that its) digital economy's share in (its annual) GDPR increased…. to 39.8 percent."); *Report on the Development of China's Digital Economy (2022)*, CHINA ACADEMY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (July 2022), http://www.caict.ac.cn/english/research/whitepapers/202208/t20220819_407677.html; Lai Lin Thomala, *Number of Internet Users in China From 2018 to 2022 with a Forecast until 2027 (in Millions)*, STATISTA (December 9, 2022), https://www.statista.com/statistics/278417/number-of-internet-users-in-china/ ("China is home to the largest online community in the world. According to estimates, the Chinese internet population was around 1.04 billion in 2022…. The country's internet penetration rate is around 72 percent, indicating that almost one out of three Chinese are still offline…. In 2022, almost all Chinese people accessed the internet through mobile phones.").

[1542] See e.g., Alina Polyakova & Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS INSTITUTION (August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/; Tiberia Dragu & Yonatan Lupu, *Digital Authoritarianism and the Future of Human Rights*, 75 INT'L ORG. 991 (2021); Fedrik Erixon & Hosuk Lee-Makiyama, *Digital Authoritarianism: Human Rights, Geopolitics and Commerce*, ECIPE Occasional Paper No. 5/2011 (2011), https://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf.

[1543] Kristen Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L. J. 317, 331 (2015) (noting that China's claim of "cyber sovereignty" is "a sovereign-based vision of Internet governance…. On the domestic front, China…. (seeks) to legitimize (its) efforts to regulate the content of the Internet available within (its territory) and to monitor and suppress expression that, in (its) view, poses a security threat"); Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMMUNICATION 3835, 3835 (2018); Anqi Wang, *Cyber Sovereignty and Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L. J. 395, 396-97, 434, 452 (2020) ["*Cyber Sovereignty and Its Boldest*"]. See *infra* Section I.B.

champions a notion of "data sovereignty" in continuation of its "cyber sovereignty" claim, striving to exert territorial-based sovereign authority over cross-border data flows.[1544]

Despite being a relative latecomer to the digital world, the PRC has now enacted a comprehensive legal and regulatory framework to regulate cybersecurity and data security, imposing strict requirements on the collection, storage, transfers, use of, and access to data collected and generated within its territory.[1545] On the grounds of cybersecurity and national security, such a data governance regime stipulates broad and expansive requirements to localize the storage and processing of different categories data within its territory by default ("data localization"), subject to limited exceptions under relatively onerous conditions.[1546] As such, data security has been increasingly ascending to a national-level policy priority of Beijing, constituting a powerful national security-based trump card constraining and even blocking transnational data flows.

Reflective of the PRC's distinct view on the relationship between cyberspace, society, and state, these aspects raise important questions for international lawyers: what accounts for China's vigorous pursuit of "cyber sovereignty" and "data sovereignty", and what do these seemingly ambiguous concepts mean exactly? How does China's domestic data governance regime evolve in its own trajectory, while being shaped by the broader Chinese political, economic, and social context? And what are the implications of this regime for the PRC's international rulemaking on cyber and data regulation?

Existing scholarship has yet to address these questions adequately. While legal literature on transnational digital governance and cross-border data flows predominantly revolves around the regulatory approaches of the EU and the U.S. (as well as their institutional arrangements for transatlantic data transfers),[1547] little ink has been spilled on China's emerging data governance regime, leaving this subject relatively undertheorized. However, in parallel to the "market-oriented" U.S. approach and the "fundamental rights-based" European approach, there arises a third paradigm featuring heavy state intervention in data governance based on security and strategic concerns in pursuit of data sovereignty.[1548] Rather than pursuing neo-liberalism policies, Western liberal values, or European fundamental rights, China's approach to data governance is driven by its distinctive political economy, reflecting the broader policy concerns and priorities of the

[1544] Matthew Erie & Thomas Streinz, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 NYU J INT'L L. POLITICS 1, 4, 26, 29-32 (2021). See *infra* Section I.C.
[1545] Rogier Creemers, *China's Emerging Data Protection Framework*, 8 JOURNAL OF CYBERSECURITY 1, 1-2 (2022) ["Emerging"]. See *infra* sections III.B and V.A.-D.
[1546] Erie & Streinz, *supra*, 29-32. See *infra* section I.C.
[1547] See e.g., Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 115 (2017). See also Paul Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALI. L. R. 877, 877 (2014); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty,* 113 YALE L. J. 1151 (2004); Richard J. Peltz-Steele, *The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation*, 19 J. INTERNET L. 1, 26 (2015); Andrew Newman, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, INT'L ORGAN. 103 (2008); ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008); HENRY FARRELL & ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY 29 (2019); Anupam Chander & Paul M. Schwartz, *Privacy and/or Trade*, 90 U. CHICAGO L. R. 49 (2023).
[1548] Creemers, *supra* (Emerging), 1-2; Susan A. Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECO. L. 245, 247, 263-68 (2018).

Chinese Communist Party (CCP) over cyberspace, the Internet, and digital information flows.[1549] Characterized by an increasing "securitisation of economic policy and economisation of strategic policy",[1550] this new regime is spearheaded by China in the international regulatory arena—another superpower that not only can disrupt global data flows by regulating its immense domestic market, but one that also enjoys a growing influence and soft power in shaping the transnational digital order.[1551]

With its increasing international influence and economic clout, China's approach to online content control and cross-border data flows may present a powerful alternative to the U.S. and the EU models that some third countries may wish to emulate, challenging Western digital governance models' perceived universality and global dominance.[1552] Given the appeal of its core tenets of governmental control, social order, and self-determined economic development,[1553] this Chinese approach to data regulation may gain immense traction particularly with like-minded developing countries amenable to the PRC's international influence. Concerned with the glaring "digital gap" in terms of digital technologies, infrastructures, capital, and talent, "Global South" countries with embryonic digital industries may find neither the American nor European models of data regulation suitable to achieve their prioritized goals of economic development.[1554] After witnessing the "Arab Spring" domestic dissidents' and human rights activists' strategic use of social media outlets to topple dictatorships and foster regime change,[1555] authoritarian regimes are generally wary of the Western-promoted "Internet freedom" agenda, sharing to varying degrees

[1549] See *infra* sections I.C, II.A.-B.
[1550] See Anthea Roberts et al., *Towards a Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECO. L. 655, 655 (2019).
[1551] Aaronson & Leblond, *supra*, 247 (2018) (arguing that the U.S, the EU, and China, as "three economic behemoths", have created three different regulatory approaches to data governance, constituting "three distinct data realms").
[1552] McKune & Ahemed, *supra*, 3840 (noting that China's claim of "Internet sovereignty has gained traction alongside (its) increasing global prominence and economic clout.")
[1553] Erie and Streinz, *supra*, 85.
[1554] See e.g., Jacquline Hicks, *Is the World's Data Being Affected by "Data Colonialism"?*, SILICONREPUBLIC (October 11, 2019), https://www.siliconrepublic.com/enterprise/data-colonialism-jacqueline-hicks-data-facebook (noting developing countries' refusal to sign up to the U.S. approach to cross-border data flows that well serves the business models of U.S. digital giants, out of strategic concerns of "structural dependency on foreign-owned digital infrastructure" and U.S. firms' "unfair share of the industry's economic benefits"); Shannon Togawa Mercer, *The Limitations of European Data Protection as a Model for Global Privacy Regulation*, 114 AJIL UNBOUND 20, 23-24 (2020) (noting that "GDPR preimplementation spending neared US$7 billion for Fortune Global 500 companies, US$1 billion for FTSE 350 companies, and millions for medium-sized companies"; and questioning whether the stringent, high-standards European data protection regulation of the GDPR is suitable for emerging and developing countries, especially given the significant costs for their local tech firms (mostly small businesses) and fledging data industries); Bhaskar Chakravorti, *Why the Rest of the World Can't Free Ride on Europe's GDPR Rules*, HARVARD BUSINESS REVIEW (April 30, 2018), https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules (arguing that "governments in the developing world should be wary of regulations as extensive as GDPR. Such regulations would impose costs on the mostly small businesses that operate in these regions and there is a sense that imposing a heavy burden on fledgling local data industries could stifle the chance for those companies to grow and compete.")
[1555] Sahar Khamis, *The Role of the Media in Arab Transitions: How "Cyberactivism" Is Revolutionising the Political and Communication Landscapes*, in IEMED. MEDITERRANEAN YEARBOOK 55-58 (2013), https://www.iemed.org/wp-content/uploads/2021/02/The-Role-of-the-Media-in-Arab-Transitions-How-Cyberactivism-is-Revolutionising-the-Political-and-Communication-Landscapes.pdf; Nahed Eltantawy & Julie B. Wiest, *Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory*, 5 INT'L J. COMMUNICATIONS 1207 (2011).

Beijing's concerns about ensuring political and social stability.[1556] Further, given Edward Snowden's revelations exposing U.S. intelligence authorities' pervasive surveillance of digital information globally,[1557] the international community's trust has been severely undermined in Washington as a global steward for unrestrained global data flows,[1558] widely raising national governments' cybersecurity concerns over foreign intelligence surveillance. For better or worse, China's regulatory approach can present an alternative model of domestic data governance for third countries to follow, building Beijing's regulatory "sphere of influence" abroad in parallel to those of Brussels and Washington.[1559]

This chapter aims to provide a contextual account on *why* and *how* China develops this regulatory approach to data governance, shedding light on the political, economic, and institutional dynamics shaping the legal and policy outcomes. Without judging the merits of this approach, it situates the rulemaking processes in the broader domestic and international political economic context, traces the evolution of data regulation in China, and considers its implications for the PRC's transnational rulemaking. As such, this contribution can help an international audience to better understand the inner logic, institutional trajectory, and operational mechanisms of China's emerging data governance regime, while avoiding the often taken-for-granted illusion of the PRC as a unitary and static monolith with single-minded pursuit of greater political control over almost everything within its reach.

The remainder of this chapter unfolds as follows. Part I explores China vision of "cyber sovereignty" and "data sovereignty", acting as the normative foundation for its domestic Internet and data governance policies. Part II analyzes the political economy underlying China's data localization measures. Part III traces the formation process of a comprehensive legal architecture governing data security and cybersecurity. Part IV outlines the centralization of Chinese cyberspace authorities mandated with online content management and data regulation. Part V reviews Chinese regulators' implementation of ancillary regulations, identifying prominent developments reflective of their regulatory focus. Part VI discusses the implications of China's domestic data governance regime for its international trade and data privacy rulemaking.

I. China's Vision of "Cyber Sovereignty" and "Data Sovereignty": The Normative Foundation for China's Domestic Digital Governance

This Part lays out the normative foundation for China's domestic digital governance. Section A discusses the CPP's longstanding concerns of regime security, leading the party-state to implement and maintain the Great Firewall to manage online content in domestic cyberspace. Section B unpacks the Chinese government's vision of "cyber sovereignty"—the normative bedrock of its

[1556] McKune & Ahemed, *supra*, 3840-41 (noting that "China, purportedly speaking on behalf of the developing world, has highlighted insufficient non-Western representation in Internet governance, the dangers of the United States as an unchallenged 'cyber hegemon,' and the inapplicability of 'Western values' in Internet sovereignty discourse. Beijing has sought to increase its influence in international forums by advancing the Internet sovereignty model as the polar opposite of 'Internet freedom,' which many governments link to the Arab Spring and efforts at regime change.")
[1557] Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, Guardian (June 9, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
[1558] Erie & Streinz, *supra*, 88.
[1559] Aaronson & Leblond, *supra*, 247.

domestic and foreign policies on Internet governance. Section C proceeds to analyze China's pursuit of "data sovereignty", which is the locus of its evolving domestic data governance regime.

A. Regime Security and the Great Firewall

As part of China's non-negotiable "core national interests", regime security (including social stability and ideological security under the broad notion of "national security") has been a perennial and prominent concern for the party-state's political leadership.[1560] Through a unique "market socialism" path towards economic modernization and industrialization,[1561] the CCP regime has developed its own political legitimacy mainly by fostering enormous, sustained economic development, without resorting to the Western model of liberal democracy.[1562] While achieving an economic take-off over the last few decades, China has remained an authoritarian party-state, with the fundamentals of its political system largely unchanged.[1563] Keen to prevent Western liberal values from gaining dominance in the domestic ideological arena, the Chinese government strives to preserve the primacy of its socialist core values (such as "patriotism", "loyalty to the communist party", and "development of a cohesive, socialist country"), in order to maintain social order, consolidate the CCP's leadership, and ensure the party-state's political legitimacy.[1564]

In the 1990s, the development of Internet technologies in the Chinese market created new politics for national information policy, exacerbating the CCP's concerns of regime stability and ideological security.[1565] While the Chinese government desired to use Internet-related information technologies to drive its economic growth and to connect to the external world, the Internet strained and challenged the CCP's capacity to maintain political control, and had potential to function as an instrument for democratizing the society.[1566]

[1560] Jinghan Zeng, Tim Stevens & Yaru Chen, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"*, 45 POLITICS & POLICY 432, 437 (2017). See e.g., The Information Office of the State Council, *The White Paper on China's Peaceful Development*, September 6, 2011. https://www.fmprc.gov.cn/web/ziliao_674904/zt_674979/ywzt_675099/2011nzt_675363/zgdhpfzbps_675409/201109/t20110906_9284881.shtml (defining China's core national interests as "state sovereignty, national security, territorial integrity, national reunification, national political system established by the PRC Constitution, overall social stability, and the basic safeguards for sustainable economic and social development."); Xi, Jinping, *Coordinating Domestic and International Situations and Laying a Solid Foundation to the Path of Peaceful Development*, PRC CENTRAL GOVERNMENT (January 2013), ("We will stick to the road of peaceful development, but will never compromise our legitimate rights or sacrifice our national core interests. No foreign country should presume that we will trade our core interests or that we will swallow the "bitter fruits" of undermining our national sovereignty, security, or development interests.").

[1561] M. J. Gordon, *China's Path to Market Socialism*, 35 CHALLENGE 53, 53 (1992) (noting that China's policy of "market socialism" was to "maintain a socialist economic system while enlarging the role of markets in the economy.").

[1562] Baogang Guo, *Political Legitimacy and China's Transition*, 8 J. CHINESE POLITICAL SCIENCE 1, 11-12 (2003).

[1563] *Id.*, 1.

[1564] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 406-7; Yun-han Chu, *Sources of Regime Legitimacy and the Debate over the Chinese Model*, 13 CHINA REVIEW 1, 26 (2013).

[1565] Milton L. Mueller, *China and Global Internet Governance: A Tiger by the Tail*, in ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 178 (Ronald Deibert et al. (eds.), 2011); Zeng, Stevens & Chen, *supra*, 437-38.

[1566] Mueller, *supra*, 177; *The Great Firewall of China: Background*, TORFOX (June 1, 2011), https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-

Due to the substantially increased scale of information dissemination and social interaction, the Internet has offered Chinese citizens with a myriad of new channels to create, access, and spread information and discourses misaligned with the government's official narratives, facilitating new forms of collective action.[1567] Notably, the occurrence of high-profile, large-scale online protest activities (sometimes together with offline collective action) deeply alarmed Chinese authorities, which grew increasingly concerned with citizens' vigorous critique of the government.[1568] Moreover, the Internet's transnational nature can enable widespread dissemination of Western liberal concepts and values (e.g., democracy, human rights, individual freedom) at odds with the CPP's mainstream political discourses, calling into question the legitimacy and accountability of the party-state.[1569] Either way, by providing novel, distributed, and efficient mediums of online content dissemination, the Internet has challenged the CCP's traditional models of centralized information control, as well as the authority of governmental propaganda institutions, while catalyzing civil dissent and mass mobilization against the state.[1570] In particular, the party-state was concerned about Internet-enabled campaigns to incite social unrest, undermine the political regime's perceived legitimacy, and foster regime-change.[1571] As a result, China was mired in an ironic dilemma: the challenge was how to embrace and leverage the economic and technological potentials brought by the Internet, while safeguarding the party-state's perceived ideological interests and political stability.[1572]

In response, since the late 1990s, the Chinese government came to adopt a massive, comprehensive, and sophisticated national Internet censorship system, commonly known as the "Great Firewall", to implement stringent online content control.[1573] As part of the Ministry of Public Security's

china-background/index.html (noting that "the Internet inherently encourages diversity of ideas, and is a tool for democratizing society.").

[1567] Mueller, *supra*, 178; Zeng, Stevens & Chen, *supra*, 438; Guo, *supra*, 1 (noting that the "telecommunication revolution has reduced people's reliance on the government-run media. The Internet has increasingly made control over the flow of information by the government more and more difficult."); Cuihong Cai, *Global Cyber Governance: China's Contribution and Approach*, 4 CHINA QUARTERLY INT'L STRATEGIC STUDIES 55, 73 (2018) ("The very nature of real-time interactivity, transnationality, anonymity and virtuality of the Internet have all provided the public with freedom of speech to the utmost extent.").

[1568] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 421-2; Guobin Yang, *Internet Activism & the Party-State in China*, 143 DAEDALUS 110, 111 (2014) ("Although hundreds of Internet protests occur every year, the main issues focus on corruption, social injustices against vulnerable persons, and abuse of power by government officials. Often, people protest because they do not trust official ac- counts of events, or because government authorities withhold information.").

[1569] Zeng, Stevens & Chen, *supra*, 438.

[1570] Gary King, Jennifer Pan & Margaret Roberts, *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 AM. POL. SCI. REV. 1, 2 (2013); *id.*, 437-38; Guo, *supra*, 1; Aaron F. Brantly, *The Cyber Losers*, 10 DEMOCRACY AND SECURITY 132, 133, 144 (2014).

[1571] Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107 (Dennis Broeders & Bibi van den Berg eds, 2020) (noting that "[f]or decades, the Chinese leadership has feared ideological subversion, and has designed online content as a potential weapon for 'peaceful evolution'.") ["Book"].

[1572] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 465-66 (noting that the Chinese authorities consider the Internet as both "an essential tool for economic growth" and "a potential threat to domestic stability and national security").

[1573] Jyh-An Lee, *Great Firewall*, CHINESE UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPERS 2018-10, at 407-8, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192725 ["Great Firewall"].

"Golden Shield Project",[1574] the "Great Firewall" refers to an overarching digital architecture constructed by the Chinese government to prevent undesirable content hosted in foreign countries from flowing into its territory via the Internet.[1575]

Unlike the decentralized networks in Western countries, China's Internet infrastructure is characterized by state-controlled "choke points" where fiber-optic cables enter the country, enabling the government to use filters and blocks to police its "digital borders".[1576] Through centralized network configuration, built-in filtering techniques, censorship software, and mandated business self-censorship, the Great Firewall functions to block domestic Internet users' access to foreign websites or mobile apps containing information that the government deems harmful to social stability and ideological security.[1577] By virtue of this mechanism, the party-state is empowered to effectively scrutinize and control digital information entering its territorial borders from overseas, striking a balance between "opening up" to the world and keeping Western ideology and liberal values away from its people.[1578]

In addition to blocking external information from abroad, the authorities also direct domestic digital platforms and Internet service providers to self-censor the Chinese Internet, filtering and removing politically sensitive online content generated from within the country.[1579] Typically amenable to the Chinese government's control and influence, Chinese Internet giants (such as Alibaba, Tencent, Baidu) have played an important role in enforcing and facilitating censorship at the behest of the party-state.[1580] In this way, as Chinese digital technologies and mobile apps increasingly interweave with Chinese people's daily life, so do the government's political control and influence.[1581]

B. Cyber Sovereignty

[1574] Lorand Laskai, *Nailing Jello to the Wall*, in CHINA STORY YEARBOOK 2016: CONTROL 194 (Jane Golley, Linda Jaivin & Luigi Tomba eds., 2017) (explaining that the "Golden Shield Project" refers to "a far-ranging attempt to harness emerging information technologies for policing").
[1575] Lee, *supra* (Great Firewall), 407-8 (noting that foreign online content deemed by censors as harmful to China "is automatically and instantaneously filtered out by the Great Firewall without the need for review or the possibility of redress."). For an explanation of the two-layered structure of the Great Firewall, see *id.*
[1576] Laskai, *supra*, 195 (noting that "for China these access points served as digital borders that needed to be controlled…. creating an effective digital veto by which the authorities could keep unwanted websites or keywords from entering the country"); Lee, *supra* (Great Firewall), 407 (noting that on the top layer of the Great Firewall, "a few state-controlled companies operate Internet-access providers and Internet-exchange points, which connect the country's domestic network to the global Internet…. By controlling the centralized network configuration and a number of key connection points or international gateways, the Chinese government can effectively control the flow of online information from abroad.").
[1577] Lee, *supra* (Great Firewall), 407-9 (noting that the government's list of prohibited content includes information that is "subversive of state power or the socialist system…. damaging national unity…. Disturbing social order…. violating the constitution or other laws."); TORFOX, *supra*.
[1578] TORFOX, *supra*.
[1579] Laskai, *supra*, 195-6.
[1580] *Id.*
[1581] *Id.*, 197.

Not surprisingly, China's Great Firewall and national censorship policies raised serious concerns from Western countries, particularly the U.S.[1582] For instance, Google, dissatisfied with China's Internet regulatory measures and censorship demands, shut down its search engine services in the mainland Chinese market in early 2010.[1583] Subsequently, then U.S. Secretary of State, Hillary Clinton, vocally advanced an "Internet freedom" agenda as a key priority of U.S. foreign policy, specifically denouncing China's censorship of the Internet as threatening the openness and freedom of cyberspace.[1584] In its 2011 *International Strategy for Cyberspace*, the White House declared its commitments to preserving core principles of free information flows and freedom of expression and association, when confronting various online challenges.[1585] A legacy of President Barrack Obama, this policy was inherited by the Trump and Biden administrations,[1586] and the EU largely shares the same view.[1587] As a pushback, the Chinese government assertively advocated for a discourse of "cyber sovereignty" (sometimes used interchangeably with "information sovereignty"), as a cornerstone of its domestic and foreign policies on Internet governance.

By definition, "cyber sovereignty" refers to the exercise of governmental control by a nation-state over the intangible cyberspace within its borders,[1588] based on its territorial jurisdiction over cyber infrastructure, Internet hardware, and software (*in rem*) and over persons engaging in cyberspace activities (*in personam*).[1589] At the core, China's conceptualization of "cyber sovereignty" consists of three distinct elements of normative substance.[1590]

[1582] Zhixiong Huang & Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271, 292, 295-6 (2017).

[1583] Bobbie Johnson, *Google Stops Censoring Chinese Search Engine: How It Happened?*, GUARDIAN (March 22, 2010), https://www.theguardian.com/technology/blog/2010/mar/22/google-china-live.

[1584] U.S. Department of State, *Secretary of the State Hillary Rodham Clinton's Remarks on Internet Freedom*, January 21, 2010, https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [Clinton Speech 1]; *Internet Rights and Wrongs: Choices & Challenges in a Networked World*, February 15, 2011, https://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm.

[1585] White House, *International Strategy for Cyberspace*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf ("States do not, and should not have to choose between the free flow of information and the security of their networks. The best cybersecurity solutions are dynamic and adaptable, with minimal impact on network performance. These tools secure systems without crippling innovation, suppressing freedom of expression or association, or impeding global interoperability. In contrast, we see other approaches—such as national-level filters and firewalls—as providing only an illusion of security while hampering the effectiveness and growth of the Internet as an open, interoperable, secure, and reliable medium of exchange.").

[1586] White House, *National Cyber Strategy of the USA*, September 2018, at 15, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; White House, *A Declaration for the Future of the Internet*, April 2022, https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf.

[1587] Huang & Mačák, supra, 296; European Commission, *New EU Cyberspace Strategy and New Rules to Make Physical and Digital Critical Entities More Resilient*, PRESS RELEASE (December 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391 (demonstrating the EU's commitments to promoting "a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.").

[1588] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 396.

[1589] Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 (1998).

[1590] McKune & Ahmed, *supra*, 3837; Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 434. While these three dimensions are concerned with on the normative underpinnings of "cyber sovereignty", the notion of "sovereignty" is multidimensional in nature. See also Creemers, *supra* (Book), 109 (identifying two major components of "sovereignty": "a normative component defining how states should conduct themselves in cyberspace" as well as "a

The first is a national defense dimension, emphasizing military and strategic cybersecurity against cyberattacks, cybercrimes, foreign intelligence surveillance, and weaponized interdependence.[1591] The second is a domestic governance dimension that empowers the government to independently adopt a national approach to Internet regulation, immune from outside pressures and foreign interference.[1592] The third is an international dimension, favoring a state-centric multilateral model for global Internet governance (as opposed to the Western-dominated private-sector-based multistakeholder model).[1593] Among them, the second dimension is not only highly controversial, but also the most relevant for cross-border information flows.

While this vision of cyber sovereignty does not directly articulate specific legal or policy prescriptions for domestic cyberspace governance, it is deployed by China as a normative justification for its policies and practices of online content control and Internet censorship, as well as an international legal basis to ward off foreign interference.[1594] By resorting to traditional public international law principles of state sovereignty and non-intervention in other countries' internal affairs, the Chinese government seeks to legitimize its domestic social management of the Internet,[1595] which is deemed essential for preserving the party-state's political legitimacy and social stability. By this virtue, China's invocation of cyber sovereignty, in effect, conditions free flows of information to the party-state's political needs to safeguard regime security.[1596]

First, under a traditional Westphalian approach to state sovereignty, the PRC asserts the final authority of the party-state as the sole arbiter of legitimate activities within its territory, enjoying absolute control over domestic political, social-economic, and cultural activities to the exclusion of external actors.[1597] Unlike Western democracies accepting restraints on national sovereignty by

---

capability component that identifies the governance and material resources and mechanisms a state requires to realize the normative component in a potentially antagonistic environment").

[1591] Ministry of Foreign Affairs, *International Strategy of Cooperation on Cyberspace*, March 1, 2017 ("no country should…. Engage in, condone or support cyber activities that undermine other countries' national security …. National governments are entitled to protect their ICT systems and resources from threats, disruption, attacks and destruction.") [*International Strategy of Cooperation on Cyberspace*].

[1592] *Id.* ("Countries should respect each other's right to choose their own paths of cyber development, model of cyber regulation and Internet public policies…. National governments are entitled to administer cyberspace in accordance with the law…. (and) to enact public policies, laws, and regulations with no foreign interference."). See *President Xi Jinping's Views on the Internet*, CHINA DAILY (December 14, 2015), https://www.chinadaily.com.cn/china/2015-12/14/content_22706973.htm (quoting President Xi's speech at the 8th US-China Internet Industry Forum in Seattle in September 2015: "China proposes that all the countries institute its own Internet policy in line with its own national conditions….").

[1593] *International Strategy of Cooperation on* Cyberspace, *supra* ("Countries should… participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony….. Cyberspace (should be) managed by all countries. International cyberspace governance should follow a multilateral approach.").

[1594] Zeng, Stevens & Chen, *supra*, 452.

[1595] *Id.*, 438-9 (noting that "[s]ince 2011-12, Internet policies have been further developed to support 'social management', a wide-ranging official concept stressing social stability, public security, and the enduring leadership of the CCP…. (which is a) response to global change that preserves the socialist ideology upon which government legitimacy is founded."). For a detailed discussion of the CCP's "social management" mechanisms, see Frank N. Pieke, *The Communist Party and Social Management in China*, 26 CHINA INFORMATION 149 (2012).

[1596] See NIGEL INKSTER, CHINA'S CYBER POWER 125 (2016).

[1597] Jacques deLisle, *China's Approach to International Law: A Historical Perspective*, 94 AM. SOC'Y INT'L L. PROC. 267, 273-74 (2000); Andrew Coleman & Jackson N. Maogoto, *"Westphalian" Meets "Eastphalian" Sovereignty: China in a Globalized World*, 3 ASIAN J. INT'L L. 237, 243-45 (2013). See Stephen D. Krasner, *Sovereignty: An*

humanitarian intervention and international human rights law after World War II, China rejects such limitations, but adopts a much more absolute conception of sovereignty, treating it as a non-negotiable "national core interest" and staunchly guarding the right to non-interference.[1598] Following the same logic, China's concept of "cyber sovereignty" likewise declines to subordinate state sovereignty in cyberspace to human rights (such as freedom of expression, freedom to information, freedom of assembly), calling for the former's undisputed supremacy against other competing norms or values.[1599]

Strategically, China advocated for "cyber sovereignty" to challenge the U.S.-promoted "information freedom" agenda favoring a global Internet free from interventionist governmental regulations.[1600] To China, the political agenda of "Internet freedom" would open the gate for importing Western values eroding the party-state's political legitimacy, thereby endangering the CCP's ideological security.[1601] Under the rubric of "cyber sovereignty", China opposes not only the applicability of universal human rights to cyberspace, but also the U.S.'s strategic moves to provide the material means to realize those rights (such as VPNs and other circumvention tools to bypass national Internet censorship).[1602] By invoking cyber sovereignty to scrutinize and control free flows of information, the Chinese government strives to shield its domestic cyberspace governance policies and practices (i.e, pervasive censorship and the Great Firewall) from international pressures, contested claims, and demands for reform, in order to secure the fundamental political interests of regime security.[1603]

Second, China and Western democracies substantially diverge in their understanding of sovereignty as applied to cyberspace, their conceptualizations of "cybersecurity", and their views on the Internet and states. While American and European authorities also increasingly recognize the importance of exercising state sovereignty in cyberspace to safeguard cybersecurity, their focus

---

Institutional Perspective, 21 COMP. POL. STUD. 66, 86 (1988) ("The assertion of final authority within a given territory is the core element in any definition of sovereignty."); STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 9 (1999) (defining "Westphalian sovereignty" as "the exclusion of external actors from domestic authority configurations."); *Cf. id.*, at 20 ("The fundamental norm of Westphalian sovereignty is that states exist in specific territories, within which domestic political authorities are the sole arbiters of legitimate behavior.").

[1598] Coleman & Maogoto, *supra*, 245; deLisle, *supra*, 274; Jerker Hellström, *Sovereignty*, in THE DECODING CHINA DICTIONARY 58 (Malin Oud & Katja Drinhausen eds., 2021), https://decodingchina.eu/ ("China insists that a country's level of development, culture and values has to be taken into account, which places strict limits on international human rights monitoring and enforcement. China tends to regard humanitarian intervention with great suspicion, arguing that it could serve as a pretext for Western countries to interfere in the domestic affairs of other states, thereby threatening their sovereignty."). See *The White Paper on China's Peaceful Development*, *supra*.

[1599] Katharin Tai & Yuan Yi Zhu, *A Historical Explanation of Chinese Cybersovereignty*, 22 INT'L RELATIONS ASIA-PACIFIC 469, 490-92 (2022) ("whereas Clinton's speech emphasized human rights dimensions of Internet freedom, in Chinese discourse human rights are widely assumed to be subordinate to state sovereignty.").

[1600] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 466. See MICHAEL JABLONSKI & SHAWN M. POWERS, REAL CYBER WAR 6-11 (2015).

[1601] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 406.

[1602] Creemers, *supra* (Book), 114-5. See Clinton Speech 1, *supra* ("We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the internet safely. The United States has been assisting in these efforts for some time, with a focus on implementing these programs as efficiently and effectively as possible. Both the American people and nations that censor the internet should understand that our government is committed to helping promote internet freedom.").

[1603] Hellström, *supra*, 58; Cai, *supra* (Global Cyber Governance), 73-4.

tends to be on infrastructure-based cybersecurity at a physical level, protecting electronic communications and critical information networks against unauthorized access, hacking, and destruction.[1604] From the perspective of technical risk management, the U.S. and the EU typically treat "cybersecurity" as the protection of confidentiality, integrity, and availability of digital information and networks.[1605]

In contrast, China's understanding of "cybersecurity" is primarily based on the potential impacts that uncontrolled flows of information may cause to political, social, or economic stability,[1606] and it often uses this concept interchangeably with "information security".[1607] While China is also a regular victim of cyberattacks, this vulnerability has not aligned its view of "cybersecurity" with the U.S. and the EU.[1608] A much broader concept than the Western version of "cybersecurity", "information security"—as understood by Chinese authorities—also encompasses, and puts emphasis on controlling information flows and censoring online content against undesirable influence, in order to secure the primacy of the party-state's ideological interests.[1609]

While many countries, including Western democracies, also censor sensitive online content for public policy or political reasons distinct to their societies,[1610] they are unlikely to support the sovereign right to conduct Internet censorship practices as extreme as China's.[1611] This is because the latter casts a far wider net, removing any information that the party-state deems to be threatening its political legitimacy and regime stability (broadly defined as "national security") as cybersecurity threats.[1612] In other words, different from the U.S. and European member states,

---

[1604] Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty*, HOOVER INSTITUTION AEGIS PAPER SERIES NO. 1703 (2017), at 3, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.
[1605] ISO Standard ISO/IEC 27032:2012, para. 4.20, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.
[1606] Creemers, *supra* (Emerging), 9; Creemers, *supra* (Book), 130 ("China primarily defines cybersecurity through the lens of "information security"…. and focuses on the potential impact the uncontrolled circulation of information might have on political, economic, and social stability"); Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST LAW REVIEW 57, 58 (2018) (arguing that "cybersecurity" under the PRC Cybersecurity Law is defined far more broadly than in the Western societies: "any digital information threatening social or political stability will be viewed as a cybersecurity, or even a national security concern.").
[1607] Segal, *supra* (*Chinese Cyber Diplomacy*), 3.
[1608] Adam Segal, *Chinese Computer Games: Keeping Safe in Cyberspace*, 91 FOREIGN AFF. 14, 15 (2012). For instance, China suffered close to 500,000 cyberattacks in 2011 alone, with almost 15% appeared to originate from U.S.-based computers.
[1609] *Id*. (noting that for Chinese policymakers, "information security" is a much broader concept that also includes regulating online content to secure ideological security in a society, in addition to the element of network security on a physical level); Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 452, 466 (noting that the Chinese government treats "inappropriate and illegal content that threatens core socialist values as both cyber and national threats").
[1610] For instance, some European countries implemented online content restrictions on Nazi symbolism to protect their social values. See JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD viii.
[1611] Tai and Zhu, *supra*, 472.
[1612] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 466. According to Chinese political leadership, its online content regulation censors "subversive", "harmful", and "malicious" content endangering national security, while welcoming "kind criticism" that contributes to a healthy online environment. As President Xi put it, "to build a well-functioned Internet public sphere is not to censor all negative comments and only endorse a single perspective; it is to welcome, investigate, and learn lessons from the kind criticism but reject those comments which turn things upside down, mix the black with the white, spread rumors with malicious intentions, commit crimes[,] and override the Constitution." But how to draw a bright line between "kind criticism" and "malicious content" remains rather unclear, but rather is arguably subject to the whims of the authorities. See *id.*, 416, 422.

China's exercise of cyber sovereignty for online content management is characterized by not only substantially different degrees of state intervention in cyberspace, but also a qualitative difference in which types of state actions are legitimate.[1613] In this sense, what makes China's interpretation and invocation of "cyber sovereignty" unique is that under this rubric, the Chinese government has been exerting unusually extensive control over online content to preserve its regime legitimacy, political security, and social stability.[1614]

At a deeper level, such divergence stems from the Chinese government's distinctive conceptualization of the Internet, largely treating it as a double-edged sword for the CCP.[1615] Similarly to Western countries, China regards the Internet as an essential tool to drive economic growth and technological advancement.[1616] Meanwhile, different from the U.S. that treats the Internet as a medium to promote personal freedom, human rights, and democracy internationally,[1617] China also considers cyber networks and information and telecommunications technology (ICT) as a potentially existential threat to the party-state's political legitimacy and national security.[1618] To put it in the words of President Xi Jinping in a high-profile 2013 speech, "the Internet has become the main battlefield of public opinions, directly impacting China's ideology security and regime security."[1619] In this context, the principle of "cyber sovereignty" is deployed by the Chinese government as a doctrinal tool to strike a balance between promoting economic development and maintaining political stability.[1620]

While the core tenets of "cyber sovereignty" began to circulate in Chinese academic and policy circles as back as the 1990s (though in a sporadic manner),[1621] this concept did not rise in political salience until very recently. Since 2010, the Chinese government started to publicly articulate the "cyber sovereignty" discourse at the international level to legitimize its approach to domestic Internet governance, and enshrined this notion as an important policy goal in top-level policy instruments and national legislations.

[1613] Tai and Zhu, *supra*, 472; Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 466 (arguing that as the way the Chinese government limits information flows differentiates itself from other democratic states, China's interpretation of cyber sovereignty is unique with regard to its content regulation dimension).
[1614] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 397, 466.
[1615] *Id.*, 466.
[1616] *Id.*
[1617] See Clinton Speeches 1, *supra* ("We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship…. Both the American people and nations that censor the internet should understand that our government is committed to helping promote internet freedom. We want to put these tools in the hands of people who will use them to advance democracy and human rights….").
[1618] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 466; Segal, *supra* (*Chinese Cyber Diplomacy*), 3.
[1619] *Xi Jinping's Speech on Internet Propaganda Work*, WENMING NET (December 25, 2021), http://www.wenming.cn/sxll/lszb/202112/t20211225_6274464.shtml (citing President Xi's speech at the national Propaganda and Thought Work on August 19, 2013). According to President Xi, the Internet is at the forefront of current ideological battlefield, and those who dominate online ideological space can safeguard a state's sovereignty and political regime. China must win the battle over online ideological space, in order to safeguard regime security at the core of national political security. See *id*.
ideology security of the Internet
[1620] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 402, 419, 466.
[1621] Mckune & Ahmed, *supra*, 3838-39.

In response to Clinton's "Internet freedom" agenda launching a high-profile diplomatic challenge to China's Internet censorship, the Chinese government published a *White Paper on the Internet in China* in 2010, marking the first time that "cyber sovereignty" received official endorsement and widespread dissemination.[1622] According to this instrument, the Internet is a critical infrastructure of a sovereignty state, the Internet network within China's territory must be under its jurisdiction, and China's Internet sovereignty should be respected and protected.[1623] And while individuals, legal persons, or other entities within China's territory enjoy the right to use the Internet, they must comply with PRC laws and regulations to protect cybersecurity.[1624]

In July 2015, the *National Security Law* referred to cyber sovereignty as an integral component of China's national security, protected by China's legal system.[1625] In November 2016, the *Cybersecurity Law* enshrined cyber sovereignty as an overarching legislative objective,[1626] providing the legal basis for the government to regulate the entire Internet.[1627] Moreover, cyber sovereignty was designated as both a fundamental principle and a key strategic goal in China's 2016 *National Cyberspace Security Strategy* and 2017 *International Cyberspace Cooperation Strategy*, respectively.[1628]

C. Domestic Data Governance in Pursuit of Data Sovereignty

As the strategic importance of data has become widely recognized in the digital era, the focus of China's domestic cyberspace regulation shifted from online content to digital information (i.e., data).[1629] Since the enactment of the 2016 *Cybersecurity Law*, the evolution of the Chinese data regulatory framework has accelerated drastically: a proliferation of national legislation, departmental regulations, and technical standards have been adopted to govern domestic data

---

[1622] Tai and Zhu, *supra*, 490 ("Although the White Paper did not specifically mention Clinton's Internet freedom agenda, it is hard not to read it as a rebuttal to the agenda laid out by Clinton, as it contained a number of specific defenses of practices specifically attacked by Secretary Clinton, most notably its extensive practice of Internet censorship.").

[1623] Information Office of the Chinese State Council, *White Paper on the Internet in China*, CHINA DAILY (June 8, 2010), https://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm ("Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security."). Here, "Internet" was used interchangeably with "cyber".

[1624] *Id.*

[1625] National Security Law, issued and effective on July 1, 2015, art. 25, http://lawinfochina.com/display.aspx?id=19663&lib=law.

[1626] Cybersecurity Law, issued on November 7, 2016 and effective on June 1, 2017, art. 1, http://www.lawinfochina.com/display.aspx?id=22826&lib=law&EncodingName=big5 (stating that the promulgation of this law is to "safeguard cybersecurity and protect cyber sovereignty and national security").

[1627] Aimin Qi, Guosong Shao & Wentong Zheng, *Assessing China's Cybersecurity Law*, 24 COMPUTER LAW & SECURITY REVIEW 1342, 1351 (2018).

[1628] State Council Information Office of the PRC, *National Cyberspace Security Strategy*, December 27, 2016, http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/39595/41105/xgzc41111/Document/1660222/1660222.htm [2016 *National Cyberspace Security Strategy*]; Department of Foreign Affairs, *International Cyberspace Cooperation Strategy*, March 1, 2017, https://www.mfa.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/201703/t20170301_7949961.shtml.

[1629] Henry Gao, *Data Regulation with Chinese Characteristics*, in BIG DATA AND GLOBAL TRADE LAW 245, 261 (Mira Burri ed., 2021) (noting China's regulation of the Internet transitioning through different phases—from the control of hardware to software, to content, and then to data); Erie and Streinz, *supra*, 85.

processing activities and to regulate cross-border data transfers,[1630] constituting the backbone of China's internal data governance regime. At the international level, China advanced the 2020 *Global Initiative on Data Security*, a proposed framework regulating data security and the digital economy, in efforts to solidify its preferred domestic norms into global standards.[1631]

Such dynamics can be best encapsulated as the rising dominance of "data sovereignty" in Chinese cyberspace governance. As an extension of the concept of "cyber sovereignty", "data sovereignty" refers to the assertion of exclusive governmental authority over the collection, storage, transfer, processing, and management of domestically generated data, establishing a bulwark against foreign governments and foreign corporations.[1632] Widely regarded by Chinese scholars as a concretization of China's "cyber sovereignty" in the data realm, this vision of "data sovereignty", in essence, applies traditional Westphalian sovereignty to the digital space, asserting the government's supreme authority to govern its domestic data to the exclusion of external powers.[1633] At the core, China's pursuit of "data sovereignty" is characterized by three major normative elements.

First, the normative premise of China's "data sovereignty" is the recognition that each state has sovereign rights and duties to protect the security of domestic data implicating its national security, public security, economic security, and social stability.[1634] From around 2012, the growing U.S.-China tech tensions[1635] and Beijing's increased concerns about terrorism at home drove Chinese authorities to attach ever greater weight to controlling online data flows.[1636] After the 2013 Snowden revelations disclosing that U.S. National Security Agency had surveilled the electronic

---

[1630] See *infra* section III.B., section V.

[1631] Chaeri Park, *Knowledge Base: China's 'Global Data Security Initiative'* 全球数据安全倡议, DIGICHINA (March 31, 2022), https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/; Shannon Tiezzi, *China's Bid to Write the Global Rules on Data Security*, DIPLOMAT (September 10, 2020), https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/.

[1632] Xuan Wu, *The Construction of Personal Information Cross-Border Transfers Rules under A Digital Sovereign Perspective*, 15 TSINGHUA LAW REVIEW 74, 75 fn.4 (2021) [吴玄，《数据主权视野下个人信息跨境规则的建构》，《清华法学》2021 年第 15 期] (arguing that the concepts of "data sovereignty" and "cyber sovereignty", at the core, apply traditional Westphalian notion of sovereignty directly to cyberspace). Chinese academics have produced a rich literature on "data sovereignty". Some scholars considered "data sovereignty" as a manifestation of national sovereignty in the digital space, and as a concretization of "cyber sovereignty" in the data realm; some defined "data sovereignty" as the supreme national powers to independently control, process, and manage national data, to the exclusion of the intervention of other countries or organizations; others argued that "data sovereignty" refers to the supreme authority of a nation-state to govern data at the domestic level, and the independent policymaking authority at the international level. See *id.* See also Erie and Thomas, *supra*, 4; Anupam Chander & Haochen Sun, *Sovereignty 2.0*, GEORGETOWN LAW FACULTY PUBLICATIONS AND OTHER WORKS. 2404, UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPER NO. 2021/041 (2021), at 1, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3422&context=facpub.

[1633] Wu, *supra*, 75 fn.4.

[1634] *Global Initiative on Data Security (Full Text)*, Sept. 8, 2020, http://www.gov.cn/xinwen/2020-09/08/content_5541579.htm [GIDS].

[1635] Creemers, *supra* (Book), 118 (noting that since 2012 "the Sino-American relationship has sharply deteriorated, most prominently through tensions concerning digital technology", and "[d]uring the second term of the Obama administration, the United States stepped up pressure against China on issues concerning cyber espionage", followed by the U.S.-China trade and tech war launched by President Donald Trump).

[1636] Creemers, *supra* (Emerging), 4.

communications of Chinese political leadership for years,[1637] China increasingly emphasized the importance of protecting national data security and cybersecurity against foreign intelligence surveillance, digital infiltration, and cyberattacks, upholding and preserving its data sovereignty.[1638]

On the other hand, as with the rapid growth of domestic ICT industry and digital economy, Chinese political leadership came to underscore the paramount role of data for economic development, technological innovation, and social governance, thereby elevating the status of data to a "fundamental strategic resource" of the country.[1639] As pointed out by the State Council's 2015 *Action Plan for Big Data Development*, "big data has become a new driving force of economic development and transformation…. ; (it) provides a new opportunity for reshaping national competitive advantage…. leading a new round of technological innovation; (and it) has become a new means of increasing the authorities' governance capacity."[1640] Thus, China committed to fully leveraging the resource of big data and strengthening its capacity to protect "data sovereignty" in cyberspace, in order to safeguard national security and enhance its international competitiveness.[1641]

Given the perceived prime importance of data as such, China has transformed the matter of data security from a primarily technical problem to a national strategic priority—namely, how to safeguard the security of its "fundamental strategic resource" against foreign and domestic hostile forces (whether public or private), while utilizing big data to achieve national informatization.[1642] Data security in cyberspace thus constitutes the protective "exoskeleton" around China's national development goals, defending its informatization process against vulnerabilities exploitable by hostile actors.[1643] In this context, national data security increasingly converges with economic

---

[1637] *NSA Spied on Chinese Government and Networking Firm*, DER SPIEGEL (March 22, 2014), https://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html ("The American government conducted a major intelligence offensive against China, with targets including the Chinese government and networking company Huawei… Among the American intelligence service's targets were former Chinese President Hu Jintao, the Chinese Trade Ministry, banks, as well as telecommunications companies….").

[1638] Huang & Mačák, *supra*, 294. See e.g., *Xi Jinping's Speech at the Brazilian National Congress*, XINHUA NET (July 17, 2014), http://www.xinhuanet.com//world/2014-07/17/c_1111665403.htm ("Although the Internet is highly globalized, the sovereignty of every country in the information sector must not be violated…. There are no double standards in the information sector, and every country has the right to preserve its information security…. A country cannot pursue its own absolute security at the cost of threatening the security of other countries."

[1639] See e.g., *Notice of the State Council on the Action Plan for Promoting the Development of Big Data*, STATE COUNCIL (August 31, 2015), Guo Fa [2015] No. 50, http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm [2015 *Action Plan for Big Data Development*].

[1640] *Id.* (stating that "big data has been playing an increasingly important role in affecting global manufacturing, circulation and distribution of products, consumption activities, various market mechanisms, social lifestyles, and national governance capacity.").

[1641] *Id.* It is in this document that the notion of "data sovereignty" made its debut in the party-state's official policy instruments.

[1642] Creemers, *supra* (Emerging), 2 (noting that China's "informatization" introduces "digital technologies in social, economic, and political life", and "is concerned with the realization of positive plans and policies that leverage digital capabilities for national development goals, which include economic growth and effective governance, applied by both the state and private actors).

[1643] *Id.*, 2.

security, social stability, public security, and even ideological security,[1644] thus constituting an indispensable part of China's national security.[1645]

Such a prioritization of "data securitization" generates two major components of "data sovereignty", one normative and one material. Normatively, "data sovereignty" empowers a government to regulate various data processing activities, and to control internal and cross-border data flows, thereby protecting data security and national security. To that end, the Chinese government increasingly implements a series of regulatory measures to manage national data security, to territorialize the storage of important or sensitive Chinese data, and to scrutinize data processing activities impinging on national security. Further, Chinese authorities also mandate the primary cyberspace regulator—*Cyberspace Administration of China* (CAC)—with centralized regulatory authority and reinforced law enforcement powers to proactively supervise and monitor data processing activities, consolidating the institutional basis to implement and enforce national legislations on cybersecurity and data security.[1646]

From a material aspect, the Chinese political leadership was acutely aware of national critical information infrastructures' heavy reliance on Western technologies, exposing vulnerabilities to foreign hostile actors (whether public or private).[1647] Specifically, China is concerned about being cut off from access to critical foreign technologies (such as semi-conductor chips), and that the dominance of U.S. tech firms may enable surreptitious installment of surveillance tools, "backdoors", or malicious code into Chinese ICT equipment at the behest of Washington.[1648] As major manifestations of "weaponized interdependence",[1649] such threats undermine China's material capacity to protect national security and achieve data sovereignty. To counter U.S. technological hegemony, China increasingly pursues technological independence, self-reliance, and autonomy (especially with respect to critical information infrastructures), which can be used not only to advance infrastructural security, but also to stimulate economic growth.[1650]

[1644] On the one hand, successful economic development is a major source of the CCP's political legitimacy. On the other hand, personal information can be hacked, misused, and manipulated by foreign intelligence operations to launch online campaigns to undercut the party-state's regime legitimacy. See *infra* Sections I.A, and II.A.

[1645] During the second collective study session of the Politburo in December 2017, President Xi stated that China must ensure its national data security, strengthen the protection of critical information infrastructures, and reinforce its capacity to safeguard important data resources of the country, which are essential for preserving national security. See *Xi Jinping: Implementing National Big Data Strategy to Facilitate the Building of Digital China*, PEOPLE'S DAILY (December 9, 2017), http://cpc.people.com.cn/n1/2017/1209/c64094-29696290.html [*Implementing National Big Data Strategy*].

[1646] See *infra* section. IV.

[1647] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 436. See *id.*, 405 (In a high-profile speech in 2016, President Xi stated that "Internet core technology is the greatest 'vital gate,' and the fact that core technology is controlled by others is our greatest hidden danger.").

[1648] Creemers, *supra* (Book), 116.

[1649] Henry Farrell & Abraham Newman, *Weaponized Globalization: Huawei and the Emerging Battler over 5G Networks*, 14 GLOBAL ASIA 8, 9-10 (2019) (discussing "chokepoint effects" and "panopticon effects" of "weaponized interdependence").

[1650] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 405; Creemers, *supra* (Book), 116 (explaining China's "indigenization strategy" that aims to increase the proportion of technology supplied by Chinese suppliers: "For both economic and political reasons, the Chinese government has increasingly sought to substitute foreign suppliers by domestic counterparts across a range of sectors."). As a context, it bears noting China's "technological indigenization" strategy. Since the Snowden revelations, China has increasingly sought to substitute foreign suppliers of information and telecommunication technology by domestic counterparts, and to increase the proportion of Chinese suppliers-

Second, based on the government's territorial jurisdiction over digital infrastructures hosting data, China's vision of "data sovereignty" underscores the supremacy of each country's exclusive jurisdiction over data generated within their own borders, as well as the sovereign right to manage national data security.[1651] Under this notion of "data sovereignty", China claims sole jurisdiction over data stored within its territorial boundary, warding off foreign governments' unauthorized access to and control of such data—whether through domestic law or intelligence surveillance.[1652]

In particular, China is wary of U.S. data hegemony.[1653] To Chinese authorities, the U.S.'s position on cross-border data flows seeks to establish a global digital order dominated by Washington and prioritizing America's economic and strategic interests.[1654] This view is exemplified by a Chinese scholar's arguments below:

> First, by promoting free data flows against foreign countries' digital trade barriers, U.S. companies can dominate foreign markets, and harvest a myriad of local personal data. Second, U.S. government can then exercise jurisdiction over such American firms to access those data. In fact, the PRISM incident is a vivid example of how the U.S. government surveilled global telecommunication data through American Internet companies. With the technological advantage of U.S. firms, the U.S. can increasingly assert "long-arm" jurisdiction. After the enactment of the U.S. CLOUD Act, American law enforcement authorities can directly request data from foreign-operating U.S. firms hosting data (i.e., data controllers), circumventing the authorities of the countries where such data are stored.[1655]

Under this view, since the U.S. can extend its jurisdiction to any location where American companies may reach, Washington is enabled to globally expand its "data sovereignty" and achieve "data hegemony", transcending the physical boundaries of national territory.[1656] According to China, such an assertion of "long-arm" jurisdiction over foreign data, exemplified

---

produced technology used in Chinese cyberspace. As evinced in the Thirteenth Five-Year Plan (2016-2020) and Made in China 2025, China has explicitly made resilience, autonomy, and self-reliance in key technologies a central goal of its national development strategy, aimed at building "an independent and advanced technology system". This trend has only intensified with the advent of U.S.-China trade and tech war, as U.S. sanctions against ZTE and Huawei vividly illustrated how China's technology was seized by the throat. See *id.*

[1651] See GIDS, *supra* ("Each country should respect other countries' sovereignty, judicial jurisdiction, and the right to manage data security").

[1652] Frequently Asked Questions, at 2, https://www.justice.gov/criminal-oia/page/file/1153466/download ("The CLOUD Act clarified that U.S. law requires that providers subject to U.S. jurisdiction disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data.").

[1653] See e.g., Linan Tian, *Countering Data Hegemony, and Strengthening the Capacity of Data Security Governance*, PRC MINISTRY OF COMMERCE (July 28, 2022) [田力男，《反对数据霸权，提升数据安全治理能力，中华人民共和国商务部（转载）》], http://exportcontrol.mofcom.gov.cn/article/zjsj/202207/698.html. This commentary was originally published in an official media outlet, Guangming Daily, and then reposted on the website of the Ministry of Commerce. See *id.* See also Congjing Ran, *Global Landscape of Data Sovereignty Governance, and China's Response*, PEOPLE'S FORUM (March 2, 2022), http://www.rmlt.com.cn/2022/0302/641108.shtml.

[1654] Wu, *supra*, 88.

[1655] *Id.* (translated).

[1656] *Id.*; Tian, *supra* ("With respect to access to data, the U.S. exercises "long-arm" jurisdiction over data stored in other countries; in terms of data sovereignty, the U.S. applies double standards; on "data diplomacy", the U.S. pursues data hegemony.").

by the U.S. CLOUD Act, is groundless and unjustified under international law, and contravenes the sovereignty of other countries.[1657] In response, China champions its vision of "data sovereignty" to challenge the global dominance of U.S. actors with respect to their unmatched capacity to collect and access data.[1658]

Notably, China opposes any foreign governments' direct requests for data located within its territory—whether from companies or individuals—without the authorization of PRC law, which are deemed to be violative of its territorial jurisdiction and data sovereignty.[1659] Regarding cross-border data transfers for law enforcement purposes, China advances a bilateral approach to deal with such needs (for instance, through bilateral agreements or traditional judicial assistance mechanisms), as opposed to a unilateral approach (embodied by the U.S. CLOUD Act).[1660] Rather than accepting a foreign law's extraterritorial jurisdiction over its domestic data, China strives to ensure its independent and exclusive sovereign powers to decide whether such data may be provided, and if so, under what conditions—based on traditional Westphalian notions of "territorial sovereignty", "non-interference" (or "independence of state powers"), and "sovereign equality".[1661]

Meanwhile, China actively denounced the practices of mass surveillance over the peoples of other countries and cyberattacks against foreign critical information infrastructures, while calling for each state to adopt preventive measures to safeguard national data security.[1662]

Regarding domestic regulatory architecture, as will be detailed later, China's 2021 *Data Security Law* mandated the establishment of a "categorized and layered" data protection system, designed

---

[1657] Tian, *supra.*
[1658] Erie and Streinz, *supra*, 85.
[1659] GIDS, *supra*.
[1660] *Id.* See Tian, *supra* (arguing that "while the arrangements of the CLOUD Act appear to be bilateral (e.g., the U.S. signed CLOUD Act agreements with the U.K. and Australia in 2019 and 2021, respectively, to facilitate mutual requests for data), such a bilateral nature is strictly limited. Different from the U.S. that can directly compel U.S. companies to provide any data collected and stored abroad, other countries, under the CLOUD Act, are subject to stringent restrictions when attempting to request for U.S.-stored data. Such states not only must satisfy more than ten strict requirements for being an eligible foreign government, but also have to pass multiple rounds of review to obtain the U.S.'s unilateral decision. Even if entering into the CLOUD Act agreement, the procedure to request for data from the U.S. is quite complex and prolonged, with the risk of being vetoed at any stage.") (translated).
[1661] Tian, *supra* (arguing that the sovereignty principle under public international law applies not only to cyberspace, but also to data, and that "data sovereignty" is a special category of "cyber sovereignty"). See *Island of Palmas* (U.S. v. Netherlands), Permanent Court of Arbitration (April 4, 1928), at 829, 838 ("Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."); *Draft Declaration on the Rights and Duties of States with Commentaries*, Text Adopted by the International Law Commission in 1949, art. 1 ("Every State has the right to independence and hence to exercise freely, without dictation by any other State, all its legal powers…."); Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, CHATHAM HOUSE RESEARCH PAPER (December 2019), paras. 33-36, https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf ("The principle of territorial sovereignty includes the right of a state to exercise jurisdiction within its own territory…. (Independence of state powers) is the (sovereign right) of states to conduct their own affairs independently as regards their own territory…. (including) the right to exercise jurisdiction…. The principle (of sovereign equality) refers to recognition in the international order of the absolute equality of all states in terms of their rights and duties in international law….").
[1662] GIDS, *supra*.

to classify and catalogue the country's "important data" and "national core data" and to provide a corresponding level of protection to safeguard national security and public interests.[1663] An innovation unseen in European or American data regulations, this system aims to increase the Chinese government's institutional capacity to manage and control domestic data that implicate national security, economic security, and public interests, thereby preventing, mitigating, and tackling potential harms and threats inflicted through data-enabled means.[1664]

Third, by invoking data sovereignty, the Chinese government moves to exercise *territorial* control over cross-border transfers of personal information and important data[1665] for commercial purposes, while imposing *extraterritorial* scrutiny on overseas data processing activities implicating its national security. When regulating domestic and overseas commercial activities involving sensitive or important Chinese data, China focuses on scrutinizing security risks, preventing the data of Chinese users and netizens from being captured as tools to surveil itself and undercut its national security.[1666] In so doing, China resorts to "data sovereignty" as an instrumental tool to balance competing interests of data security and economic development, using its own policy preferences to reshape cross-border data flows.

In the aftermath of Snowden revelations, Chinese authorities, having realizing that the treatment of personal data increasingly triggered national security, rapidly imposed data local storage requirements in numerous sectors, including banking, healthcare, mapping, Internet publishing, online ride-hailing, cloud services, among others.[1667] Such legislative efforts culminated with the 2016 *Cybersecurity Law*, which for the first time stipulated horizontal data localization requirements on critical information infrastructures for national security purposes.[1668] In a similar vein, the 2021 *Personal Information Protection Law* provided comprehensive localization conditions for personal information held by data controllers triggering the CAC's prescribed volume thresholds.[1669] After that, this trend continued and went granular, with more sector-specific measures adopted to regulate sensitive sectors.[1670] Highly controversial to the international business community, these regulatory measures of data localization are perceived by Chinese authorities as necessary and conducive to achieving data security against foreign governments' mass surveillance, as they may constrain the latter's ability to collect and access data generated in China.[1671]

While these data localization measures do not strictly prohibit data export *per se*, they make cross-border data transfers the exception, rather than the rule. To enable cross-border data transfers and facilitate international digital trade, Chinese regulators came up with three data export mechanisms for companies to deploy, including security assessments, certification, and standard contractual agreements. Albeit with different compliance requirements and regulatory specificities, these mechanisms share a common policy focus: namely, to preserve national data security against

[1663] See *infra* Section III.B.(D).
[1664] Creemers, *supra* (Emerging), 1, 6-7.
[1665] For a discussion on the concept of "important data", see *infra* Sections III.B.(A), V.B., and V.D.
[1666] Tian, *supra*.
[1667] Creemers, *supra* (Emerging), 4. See *infra* section III.A.(A).
[1668] See *infra* section III.B.(A).
[1669] See *infra* section III.B.(B).
[1670] See *infra* section V.B.
[1671] See *infra* section II.B.

unauthorized collection by foreign private and public actors. Though opening an institutional alternative to data localization, these mechanisms are subject to relatively onerous conditions, limitations, and constraints, and thus, are unable to override the default settings of localized data storage.[1672]

Beyond cross-border data transfers between data exporters and importers, the Chinese government also increasingly scrutinized transnational business transactions that may bring masses of domestic data under the jurisdiction of a foreign government, including foreign listing and corporate structuring.[1673] By deploying the data security review mechanism to screen potential national security risks, the Chinese government becomes more assertive in regulating the local effects of extraterritorial data processing activities,[1674] extending its regulatory control to international corporate transactions implicating sensitive and important Chinese data. As suggested by this notable development, China's domestic data governance regime has been expanding its domain and frontier over time, and a constant theme tends to be guarding large troves of domestic data against unwarranted access and control by foreign governments, particularly the U.S.

II. THE POLITICAL ECONOMY UNDERGIRDING CHINA'S DATA LOCALIZATION MEASURES

Having surveyed the normative underpinnings of "cyber sovereignty" and "data sovereignty", this Part turns to the salient political, economic, and strategic motivations driving China's data localization measures. Among them, what stand out are the party-state's twin goals: protection of national security interests (a primary and perennial concern) and development of digital industry and technologies (secondary, yet increasingly important).

A. Protection of National Security Interests

Under China's vision of cyber sovereignty, cyberspace is the "fifth domain" subject to its territorial sovereignty (along with Land, Sea, Air, and Space),[1675] and the Internet is essentially a state-owned telecommunication infrastructure.[1676] Despite its substantial potential in boosting economic growth, the Internet could be weaponized by hostile forces (public or private, foreign or domestic) to undermine the political legitimacy of a socialist regime. According to the CCP's political leadership, the Internet is perhaps one of the biggest threats to national ideological security, given its pervasive influence in shaping Chinese people's understanding about the legitimacy of a political regime.[1677] Compared with the associated commercial interests (which are indeed important), the political and ideological security of the ruling regime is deemed the foundation of

[1672] See *infra* section V.A.(C).
[1673] See *infra* sections V.C, and V.D.
[1674] Goldsmith, *supra*, 476 (arguing that "[t]erritorial sovereignty (over the Internet) supports national regulation of…. the local effects of extraterritorial acts.")
[1675] 2016 *National Cyberspace Security Strategy*, *supra*.
[1676] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 402.
[1677] See *supra* section II.B. See e.g., *General Secretariat Xi Jinping Instructs the Building of a Clean Cyberspace*, COMPUTER NETWORK INFORMATION CENTER (March 21, 2022), http://cnic.cas.cn/jdtw/202203/t20220321_6401853.html (quoting a statement made by Xi Jinping in a 2013 Conference on National Ideological Work: "Whether We can prevail in the battlefield of the Internet determines China's ideological and regime stability").

various economic activities on the Internet.[1678] Based on this conceptualization, China instrumentalizes the notion of "cyber sovereignty" to exert stringent regulatory control over the Internet, online activities, and data for national security purposes, while utilizing information technologies to spur the development of the digital economy.[1679]

For Chinese policymakers, this "double-edged" conceptualization of the Internet likewise applies to data. As considered by Chinese authorities, while data indeed constitutes a crucial resource for economic development and technological innovation, data, first and foremost, can become a source of vulnerability for the CCP's regime, endangering its cybersecurity and national security.[1680] Though China prioritizes both development and security, data security—as an important component of national security—is a non-negotiable bottom-line.[1681]

Territorializing the storage and processing of sensitive and important domestic data (including personal information) is an inherent part, a continuation, and a concrete manifestation of China's "cyber sovereignty". Otherwise, unconstrained flows of data across borders may render Chinese authorities' control, filtering, and censoring of online information overly cumbersome and less manageable, undercutting the party-state's perceived national security interests (including regime stability and ideological security).

Moreover, given the increasing overlap between data security and national security, Chinese authorities' regulatory decision to localize the storage and processing of certain categories of data is largely driven by the motivation to safeguard the security of domestically originated data against vulnerabilities that hostile forces may exploit, especially against antagonistic foreign governments with unparalleled signal intelligence and cyberwarfare capacities. The below outlines a typical, non-exhaustive set of scenarios, whereby the access to and control of personal data held in a country can generate national security risks—yet the same may also occur with various non-personal data (such as government data, business data, telecom data, traffic data, geographic data, environmental data, military data, among others).

First, large amounts of personal information—especially those of politicians, officials, military—may be hacked or misused by foreign enemies or terrorists to commit crimes, espionages, and political infiltrations, thus undermining a state's security interests.[1682] Meanwhile, if crossed with

---

[1678] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 402.
[1679] *Id.*
[1680] See e.g., *Encouraging Legal, Reasonable, and Effective Use of Data, and Providing Basic Legal Safeguard for Data Security*, National People's Congress of the PRC (December 8, 2021), http://www.npc.gov.cn/npc/c30834/202112/e7ec3ff977f64e63ac6033aaa83b8d92.shtml ("Implementing a holistic national security view: As emphasized by President Xi, Jinping, 'We must apply national security throughout all aspects of the CCP and the government's work…. stick to a systematic thinking, and construct a holistic national security view.' *Data security is an important part of national security*…. China will…. accelerate the development of the digital economy, *while firmly guarding the bottom line of data security*.") (emphasis added). This article was originally published in an official media outlet, People's Daily, and then reposted on the website of the National People's Congress. See *id.*
[1681] *Id.*; Tian, *supra*. See *supra* chapter 1 ("A Battle of the Big Three"). Section II.C. (explaining China's dominant security-oriented conceptualization of personal data with respect to TPDF regulation).
[1682] See Josie Le Blond, *German Politicians' Personal Data Leaked Online*, THE GUARDIAN (January 4, 2019), https://www.theguardian.com/world/2019/jan/04/german-politicians-personal-data-hacked-and-posted-online; Sarah

other data sets and processed by algorithms, even seemingly innocuous troves of anonymized personal data may be deanonymized and weaponized, revealing the government's classified information, sensitive policy objectives, and military strategies.[1683]

To illustrate China's understanding of how vast amounts of personal information held by private-sector actors may implicate national security, it is worth noting a telling example given by Dr. Yanqing Hong—a Chinese scholar who led the drafting of China's cross-border data flow regulations. As argued by Hong:

> The huge amount of user information held by Alibaba, currently over 400 million, is certainly personal information…. but because of its scale and granularity, it can also match the public security organs' basic national population database and even surpass it in accuracy. For the country, any eventual leak or damage of this scale of basic population data could create a serious threat to national security.[1684]

Second, for a nation-state, relying on foreign firms to provide ICT services and products for its private and/or the public sectors risks creating "weaponized interdependence", since the data collected within its borders can be transferred to the home country, whose government may access and amass such data through intelligence surveillance or domestic law.[1685] As suggested by Snowden revelations, foreign communication infrastructures and applications can be turned into a surveillance tool, or a machine for espionage, imposing imminent threats to a host state's national security.[1686]

Third, by harvesting and misusing large troves of personal data, foreign intelligence operations may systematically spread tailor-made online misinformation to targeted audiences through social networks or online media.[1687] In this way, masses of personal information can be exploited and weaponized by foreign hostile forces to manipulate domestic public opinions, and influence the general public's perceptions of the legitimacy of a political regime, thus eroding the domestic political leadership's perceived ideological interests and regime stability.[1688]

Albrycht, *When the Homefront Becomes the (Cyber) Front Line*, FIFTH DOMAIN (February 3, 2020), https://www.fifthdomain.com/opinion/2020/02/03/when-the-homefront-becomes-the-cyber-front-line/.

[1683] Susan Ariel Aaronson, *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*, CIGI PAPER NO. 241 (April 15, 2020), at 3, https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves/; Yanqing Hong, *The Cross Border Data Flows (Data Exit) Security Assessment: An Important Part of Protecting China's Basic Strategic Resources*, RESEARCH ALLIANCE FOR DATA GOVERNANCE AND CYBER SECURITY (January 4, 2018), http://www.dgcs-research.net/a/Opinion/2018/0103/59.html (noting that "hostile forces could combine the data with other datasets and use various analysis methods such as data mining to gain information that could threaten national security.") [*Data Exit*].

[1684] Hong, *supra (Data Exit)*.

[1685] Farrell & Newman, *supra* (*Weaponized Globalization*), 9-10.

[1686] *Id.*, 10.

[1687] See Adrian Chen, *Cambridge Analytica and Our Lives Inside the Surveillance Machine*, THE NEW YORKER (March 21, 2018), https://www.newyorker.com/tech/annals-of-technology/cambridge-analytica-and-our-lives-inside-the-surveillance-machine; Jane Mayer, *New Evidence Emerges of Steve Bannon and Cambridge Analytica's Role in Brexit*, THE NEW YORKER (November 17, 2018), https://www.newyorker.com/news/news-desk/new-evidence-emerges-of-steve-bannon-and-cambridge-analyticas-role-in-brexit.

[1688] See Tian, *supra*.

These aspects exemplify national security risks imposed by data—particularly, personal information. This explains why Chinese authorities increasingly emphasized the necessity of data localization to safeguard data security and cybersecurity.[1689] Given the party-state's priorities of national data security and regime security, it not surprising that China implements strict regulatory measures to control cross-border data transfers, as with its practices of censoring online information. When regulating data export as such, the focus of Chinese authorities is to scrutinize security risks imposed by private and public actors in the recipient country, especially foreign intelligence surveillance. Even if complete protection against these threats is impossible, data localization can make it more difficult and expensive for foreign hostile forces to gather data from China and conduct activities harmful to its national security,[1690] particularly given the PRC's burgeoning domestic cybersecurity industry with increasingly competitive capacity.[1691]

B. Development of Digital Industry and Technologies

While the primary objective of Chinese cyber governance policies and data localization measures is to protect national security interests, the implementation of such regulations has created externalities benefiting Chinese tech firms and digital industry, at the cost of their foreign competitors. Such an ancillary effect was realized by Chinese authorities, when foreign trading partners—most notably, the U.S. and the EU—complained about adverse impacts brought on their businesses and labeled Chinese measures as "protectionist". But on its part, China, of course, is unwilling to subordinate its cyber and data sovereignty to foreign commercial interests, even at the cost of suffering certain economic losses. This is because Chinese authorities perceive national security as a non-negotiable "national core interest". Further, the self-serving economic impacts are not inconsistent with China's industrial policy goals to nurture domestic champions, develop the digital economy, and dominate cutting-edge technologies. Thus, Chinese authorities welcome such externalities of its domestic cyber and data regulations, hoping to utilize big data to achieve broader economic and strategic goals in the global tech race.[1692]

Though focused on filtering information for political reasons, the Chinese government's stringent censorship of online content and selective blocking of sensitive foreign websites may constitute an important trade barrier for multinational companies operating in China. Notably, the operation of the Great Firewall may restrict or ban access to websites, digital tools, and services located on overseas servers, which is often a prerequisite for foreign companies to deliver web-based digital

---

[1689] Anthea Roberts et al., *Geoeconomics: The Chinese Strategy of Technological Advancement and Cybersecurity*, LAWFARE (December 3, 2018), https://www.lawfareblog.com/geoeconomics-chinese-strategy-technological-advancement-and-cybersecurity.

[1690] John Selby, *Data Localization Laws: Trade Barriers or Legitimate Response to Cybersecurity Risks, Or Both?*, 25 INT'L J. L. INFO. TECH. 213, 228, 231-32 (2017) (arguing that data localization requirements can lessen the competitive advantage of the U.S. in conducting Internet signals intelligence surveillance as compared with other countries, making it more expensive for its National Security Agency to operate "as wide-spread mass surveillance on the citizens of other countries as it currently does.").

[1691] See Giulia Interesse, *China's Cybersecurity Industry: A Market Analysis*, CHINA BRIEFING (October 26, 2022), https://www.china-briefing.com/news/chinas-cybersecurity-industry-a-market-analysis/ ("In recent years, with the continuous improvement of China's information technology sector and growing emphasis on data protection, the domestic cybersecurity market has rapidly matured. There are many enterprises providing network security products, with different models, fierce market competition, and low concentration.").

[1692] Jinhe Liu, *China's Data Localization*, 13 CHINESE J. COMM. 84, 92-93 (2020); Creemers, *supra* (Book), 125. See *supra* section I.C.

or physical products to Chinese consumers and businesses.[1693] Meanwhile, routing Internet traffic through a national firewall can delay information transmission in ways that considerably degrade the quality of the services rendered—sometimes, even to a commercially unacceptable level—thus precluding or inhibiting transnational flows of certain digital products.[1694] In effect, China's Internet filtering measures can create an uneven playing field to the disadvantage of foreign firms, while indirectly supporting the growth and success of Chinese digital firms.[1695]

Likewise, China's data localization measures would raise the costs for multinational companies to conduct business in the Chinese market, tilting the playing field to their disfavor. First, by imposing restrictive and onerous conditions for cross-border data transfers,[1696] such regulations, in effect, compel foreign digital firms to build or purchase domestic data storage capacities in China.[1697] Due to related time delays, extra costs, and legal uncertainties inherent in using China's data export mechanisms, foreign data-intensive businesses may have to establish and maintain local physical infrastructures (e.g., data centers) to store and process data generated in China.[1698] In contrast, free data flows would permit multinational firms to serve the Chinese market with much less of a physical presence.[1699]

Second, sweeping data localization requirements and restrictions on cross-border data flows may reduce imports of data-intensive services from abroad, adversely affecting the price and quality of online services provided by foreign firms operating in China.[1700] Also, such measures may hinder a range of data-intensive services (including computing, retail, and information services) from being directly traded over the Internet, but rather may demand foreign firms to supply such services through the establishment of a commercial presence in China.[1701]

[1693] Shamel Azmeh & Christopher Foster, *The International Trade Regime and the Quest for Free Digital Trade*, 22 INT'L STUDIES REV. 1, 7 (2019). See Lee, *supra* (Great Firewall), 408 (noting that the Great Firewall not only can block domestic users from accessing unwanted foreign websites, but also may disrupt the function of available circumvention tools—though it is possible to use virtual private networks (VPNs) to get around the Great Firewall, such tools may occasionally fail to fully function due to the continuous upgrades of the latter).

[1694] USTR, *2017 National Trade Estimate Report on Foreign Trade Barriers*, at 90, https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf. See Lee, *supra* (Great Firewall), 408 (noting that in addition to blocking foreign websites containing prohibited information, the Great Firewall's presence can make some foreign websites unable to function at normal speed).

[1695] Cynthia Liu, *Internet Censorship as a Trade Barrier: A Look at the WTO Consistency of the Great Firewall in the Wake of the China-Google Dispute*, 42 GEORGETOWN JOURNAL OF INTERNATIONAL LAW 1199 (2011).

[1696] See *infra* Sections III.B. and V.A.

[1697] Azmeh and Foster, *supra*, 7.

[1698] *Id.*; Erie and Streinz, *supra*, 31-32. See *infra* Section V.A.(C).

[1699] Sveltlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV., 416, 472-73 (2020); U.N. Conference on Trade and Development, *World Investment Report: Investment and the Digital Economy*, UN Doc. UNCTAD/WIR/2017 (June 7, 2017), at 167, https://unctad.org/system/files/official-document/wir2017_en.pdf.

[1700] Martina F. Ferracane and Erik van der Marel, *Do Data Policy Restrictions Inhibit Trade in Services?*, ECIPE Digital Trade Estimates Working Paper No. 2, 2018, at 15, https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf ("more restrictive data policies, in particular with respect to the cross-border movement of data, result in lower imports in data-intensive services for countries imposing them"); Martina F. Ferracane & Erika van der Marel, *The Cost of Data Protectionism*, ECIPE (October 2018), https://ecipe.org/blog/the-cost-of-data-protectionism/ ("if countries lifted their restrictions on cross-border flow of data, the imports of services would rise on average by five percent across all countries, with obvious benefits for local companies and consumers who could access cheaper and better online services from abroad").

[1701] Ferracane & van der Marel, *supra* (*The Cost of Data Protectionism*).

Third, data localization measures often undermine the economic efficiency of multinational firms' global operation by forcing them to adopt a less efficient mode of production (or supply) of services.[1702] In the modern economy, personal data has become an important factor of production—not only for ICT services, but also for trade in goods and services in general.[1703] Notably, personal data of customers and users have become an important ingredient of algorithms and AI-based systems, as well as a crucial input for many digital services, manufacturing processes, targeted marketing practices, and logistics operations.[1704] Under restrictive data export regulations that constrain their control and use of data, foreign companies would be placed in a less favorable position to compete in China, compared with Chinese firms that need not comply with such requirements to provide the same goods or services domestically.[1705]

Given these aspects, China's trading partners and foreign industry groups have expressed strong concerns about the trade distortive effects of its data localization measures and cross-border data transfer restrictions, calling them "barriers to digital trade" and part of a protectionist trade policy.[1706] While recognizing such externalities, China not only continued to implement its domestic data governance regime without substantial change, but also strengthened the efforts to develop and promote its digital industry, in order to increase its ability to effectively compete in the international digital arena.

First, China's data localization requirements not only demand the relevant data to be stored and processed in China, but also address the issue of "by whom".[1707] Since the operation of data center services require a special license that is currently unavailable to foreign-invested companies, foreign cloud service providers need to co-operate on a contractual basis with licensed Chinese companies to supply such services in China.[1708] For instance, to comply with PRC regulatory requirements, Apple had to store the personal data of its Chinese iCloud users on computer servers

---

[1702] Yakovleva, *supra*, 472.
[1703] *Id*.
[1704] *Id*., 471.
[1705] *Id*., 471-73.
[1706] See eg. USTR, Fact Sheet on the 2020 National Trade Estimate, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade (listing China's data localization requirements and restrictions on cross-border data flows as key barriers to digital trade); USTR, U.S. Statement on the Trade Policy Review of China, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/us-statement-trade-policy-review-china; American Chamber of Commerce in Shanghai, *Navigating China's Data Maze: How Regulations Affect U.S. Companies*, VIEWPOINT (May 2019), at 7, https://www.amcham-shanghai.org/sites/default/files/2019-05/Viewpoint%20-%20Data%20%28May%202019%29.pdf; European Chamber, *European Chamber Stance on China's Data Security Law and Personal Information Protection Law*, PRESS RELEASE (August 25, 2021), https://www.europeanchamber.com.cn/en/press-releases/3367/european_chamber_stance_on_china_s_data_security_law_and_personal_information_protection_law.
[1707] Erie and Streinz, *supra*, 22.
[1708] Samuel Yang, *Regulation of Cloud Computing in China*, CHINA LAW VISION (October 13, 2020), https://www.chinalawvision.com/2020/10/intellectual-property/cybersecurity/regulation-of-cloud-computing-in-china/ ("as (internet data center (IDC)) services were not part of the scope of (value-added telecoms services) to be opened up to foreign investment that China made at its accession to the WTO on 11 December 2001, IDC licences have only been granted to Chinese companies and their joint ventures with Hong Kong and Macau investors, and not to companies invested in by investors from other jurisdictions").

run by a Chinese partner company in Guiyang.[1709] As such, China's data localization measures are deployed as part of an industrial policy to promote domestic digital industry, forcing multinationals to invest in China and co-operate with Chinese firms for rendering data hosting services.[1710]

Second, despite China's unwavering pursuit of data sovereignty to secure national security, as noted earlier, Chinese political leadership increasingly embraces "big data" as a "fundamental strategic resource" to achieve informalization, while pledging to utilize it to reshape the country's competitive advantage.[1711] In this regard, a review of China's top-level policy instruments reveals the party-state's growing emphasis on exploiting the economic utility of big data, though protecting national security remains its perennial and paramount concern.

In the 2015 *Action Plan for Big Data Development*, China recognized big data as a new force driving economic and technological transformation, while undertaking to make full use of its "data scale advantage" to strengthen its international competitiveness.[1712] During the *second collective study session of the Politburo* in December 2017, President Xi called on the central government to spur the development of big data technologies, and to build a digital economy driven by data as an engine for innovation.[1713] In the *Fourteenth Five-Year Plan for Big Data Industry Development*, China underscored the role of data as an important "factor of production" for developing the digital economy, and prioritized the growth of the big data industry as an engine to transform national economic development.[1714] And the State Council approached China's "massive data resource" as an unique advantage for the development of AI,[1715] which is widely regarded as the next battlefield of global tech competition.

These statements indicate China's acute awareness of the economic effects of big data, and its realization that this dimension presents it with unprecedented opportunities in the global geo-political and -economic competition. By treating data as a "fundamental strategic resource", Chinese authorities alluded to the paramount importance of data in developing the digital economy and transformative technologies, which is deemed essential to foster "an independent and

---

[1709] Jack Nicas et al., *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, NEW YORK TIMES (June 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

[1710] See Azmeh and Foster, *supra*, 7-8.

[1711] See e.g., Ministry of Industry and Information Technology, *Development Plan for the Big Data Industry (2016-2020)*, December 18, 2016, https://www.miit.gov.cn/jgsj/xxjsfzs/zlgh/art/2020/art_fa5c0abf3c7442cb89fcf37d8f311aa6.html; Hong, *supra* (*Data Exit*) ("'Data has become a national basic strategic resource.' This is the common understanding of the two basic official documents which are guiding China's future economic and social development: The Action Plan to Promote the Development of Big Data and the 13th Five-Year Plan."). See also *supra* Section I.C.

[1712] 2015 *Action Plan for Big Data Development*, *supra.*

[1713] *Implementing National Big Data Strategy*, *supra*.

[1714] Ministry of Industry and Information Technology, *Fourteenth Five-Year Plan for Big Data Industry Development*, http://www.gov.cn/zhengce/zhengceku/2021-11/30/5655089/files/d1db3abb2dff4c859ee49850b63b07e2.pdf. Data was first labeled as a new "factor of production" in the Fourth Plenary Session of the Nineteenth Central Committee of the Communist Party of China in October 2019, see https://www.ndrc.gov.cn/wsdwhfz/202208/t20220831_1334891.html?code=&state=123.

[1715] *Notice of the State Council on the Development Plan of New-Generation Artificial Intelligence*, STATE COUNCIL (July 8, 2017), Guo Fa [2017] No. 35, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm ("China should firmly grasp the major opportunities brought by the AI development…. secure a head start and lead the world's AI development…. in order to serve China's social and economic development, support national security, and rapidly strengthen China's international competitiveness.").

advanced technology system" and to boost its national core competitiveness internationally.[1716] Given the unique role of data as a factor of production and an input for AI development, localization of data may provide an immense economic advantage to Chinese firms over their Western peers. Notably, such a policy could enable China to better utilize this strategic asset to develop self-reliant innovation capacity, to ascend up global value chain, and to secure a head start in mastering cutting-edge technologies.[1717] Meanwhile, data localization requirements would make it difficult to export China's fundamental strategic resource to the U.S. and other western countries, preventing such data from being turned into their assets in the global tech rivalry.[1718] These factors can bolster the competitive advantage of China and Chinese firms in the U.S.-China tech race—particularly, in the battle to dominate AI.[1719]

****

From a political economic perspective, China's national security interests have been paramount, acting as an overarching objective undergirding China's domestic Internet governance and data regulatory policies. Meanwhile, the economic and strategic goals identified have increasingly risen in importance, and come to supplement, rather than replace, China's dominant security concerns. As evinced from President Xi's dictum—"there will be no national security without cybersecurity, and no modernization without informatization", and "cybersecurity and informatization are just like two wings of a bird, or two wheels driven by one engine"[1720]—such two sets of forces are often intertwined, and, in some cases, mutually reinforcing.[1721]

For China, national security is a non-negotiable national core interest, and an indispensable precondition for achieving informatization. On the other hand, progress in the informatization process can solidify the party-state's material capacity, boost national economic growth (a pillar of the CCP's political legitimacy), and reinforce China's international competitiveness, thereby strengthening national data security and cybersecurity.[1722] In fact, both cybersecurity (encompassing data security) and informatization are two integral components for making China a "cyber superpower" (*wangluo qiangguo*), as envisioned by President Xi in 2014.[1723] Combined

---

[1716] See Creemers, *supra* (Book), 116-18; Liu, *supra* (*China's Data Localization*), 92-93.
[1717] Roberts et al., *supra* (*Geoeconomics*).
[1718] *Id*.
[1719] *Id.*
[1720] *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, February 27, 2014, http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm.
[1721] Roberts et al., *supra* (*Geoeconomics*).
[1722] See Creemers, *supra* (Book), 125 (noting that "with a growing priority of cybersecurity", China's "informatization" efforts (including industrial policy and investment to raise the domestic capabilities of its digital industry) "combine the imperative of *economic development* with *a political goal: domestic (business) players are seen as more secure and amenable to government control than foreign businesses*.") (emphasis added).
[1723] *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, *supra*; Creemers, *supra* (Emerging), 2 ("In 2014, Xi Jinping announced a drive to turn China into a "cyber power"…. through the combination of informatization, the introduction of digital technologies in social, economic, and political life, and cybersecurity. In other words, informatization is concerned with the realization of positive plans and policies that leverage digital capabilities for national development goals, which include economic growth and effective governance, applied by both the state and private actors. Cybersecurity, in turn, forms the protective exoskeleton around this sphere of development, defending against vulnerabilities that hostile actors might exploit.").

together, these political and economic objectives account for the major motivations underlying China's data localization measures.

III. CHINA'S LEGISLATIVE FRAMEWORK GOVERNING DATA SECURITY AND CYBERSECURITY

This Part proceeds to analyze the legislative framework forming the backbone of China's domestic data governance regime, focused on the regulation of transnational data flows. Overall, the development of this framework went through two phases. From the 1990s to 2016, the regulatory landscape was characterized by sectoral laws and regulations imposing sector-specific personal information protection and data localization requirements (Section A). After the adoption of 2016 *Cybersecurity Law* as a watershed, Chinese authorities intensified their legislative efforts to construct a comprehensive data governance framework (Section B). With *Cybersecurity Law*, *Personal Information Protection Law*, and *Data Security Law* in place, the basic institutional structure of China's data governance regime has taken shape, tightening the government's regulatory control over domestic data processing activities and cross-border data transfers.

A. Legislations and Regulations From the 1990s to 2016

Unlike major industrialized democracies that had enacted data privacy protection laws to respond to risks brought by computerized data processing since the 1970s, protection of privacy or personal data had long been a legislative void under China's legal system.[1724] Yet, with the development of the Internet industry in China by the late 1990s, legislatures and regulations specifically protecting personal information began to emerge slowly.[1725] Before the 2016 *Cybersecurity Law*, China largely adopted a sectoral regulatory approach to personal information protection, with the relevant provisions dispersed among numerous sectoral laws and regulations.[1726] Under this piecemeal approach, restrictions on cross-border data transfers showed up until very recently. Scattered in different sectoral regulations, these fragmented rules of data localization were enforced and implemented by the relevant sector-specific regulators with no centralized coordinating authority.[1727] The below identifies major sectoral rules governing this matter during this stage.

In 2011, the People's Bank of China (a central financial regulatory authority in the banking sector) promulgated a notice on the protection of personal financial information protection, marking the first sectoral regulation by the Chinese government for the local storage of personal data.[1728] Under this instrument, financial institutions must localize the storage and processing of personal financial

---

[1724] Raymond Yang Gao, *Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era*, 13(1) TSINGHUA CHINA LAW REVIEW 165, 167 (2020).
[1725] *Id.*
[1726] *Id.* Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PENN. ST. J. L. & INT'L AFF. 49, 70-78 (2020) (detailing China's "initial preference for the minimalist approach" to personal data protection).
[1727] Keming Cai, *Jurisdictional Report: People's Republic of China*, in REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 73 (Clarisse Girot ed., 2018), https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/# [*Jurisdictional Report*].
[1728] Liu, *supra* (*China's Data Localization*), 89. See *Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Financial Institutions in the Banking Sector*, [2011] No. 17 of the People's Bank of China, issued on January 21, 2011, effective on May 1, 2011, http://www.lawinfochina.com/display.aspx?lib=law&id=8837&CGid= [2011 PBOC Notice].

information that they obtain in the course of their business.[1729] In 2015, there emerged new regulations that required credit reporting agencies to store and process personal financial information in China, and which demanded bank card clearing institutions to use China-based financial infrastructure to process domestic bank card clearing business.[1730] These data localization requirements are mainly driven by the motivation to protect the security of the national financial system against potential hostile forces, which is deemed essential for cybersecurity and national security.[1731]

In 2014, the National Health and Family Planning Commission issued the *Interim Measures for the Governance of Population Health Information*,[1732] aimed at strengthening regulation on the collection and use of public health data (including personal health data and aggregated population health data).[1733] Under this regulation, all medical and health institutions must store population health information in servers located in China, and shall not use any foreign servers to process such data.[1734]

In 2015, the State Council issued a *Regulation on Map Management*, requiring online map service providers to store map data in servers located in China and to implement data security protection measures.[1735] In 2016, newly enacted regulations on Internet publishing, online ride-hailing, and cloud services demand these service providers to use China-domiciled servers, and to domestically store the data processed in the course of their business.[1736]

Overall, the promulgation of these regulations evinces Chinese authorities' increasing national security concerns over data-inflicted vulnerabilities in the country's economic, technological, and social systems available to foreign hostile actors, driving the government to tighten regulatory control over select sensitive data. However, the effects of these regulations enacted at this stage were rather limited in practice, with most cross-border data transfers (other than those concerning state secrets) from China largely unregulated.[1737] This status quo is due to the relatively weak

---

[1729] 2011 PBOC Notice, para. 6. "Personal financial information" includes personal information that concerns the customers' identity, property and income, banking accounts, credit, financial transactions, among others. See id., para. 1.
[1730] Cai, *supra* (*Jurisdictional Report*), 69.
[1731] *Id.*
[1732] *Notice of the National Health and Family Planning Commission on Issuing the Measures for the Governance of Population Health Information (for Trial Implementation)*, [2014] No. 24 of the National Health and Family Planning Commission, issued and effective on May 5, 2014, http://www.lawinfochina.com/display.aspx?id=17535&lib=law [Interim Measures on Population Health Information].
[1733] Cai, *supra* (*Jurisdictional Report*), 71.
[1734] Interim Measures on Population Health Information, arts. 3, 10.
[1735] *Regulation on Map Management*, Order of the State Council No. 664, issued on November 26, 2015, effective on January 1, 2016, art. 34, http://www.lawinfochina.com/display.aspx?id=21392&lib=law.
[1736] *Provisions on the Administration of Online Publishing Services*, issued on February 4, 2016, effective on March 10, 2016, art. 8(3), http://lawinfochina.com/display.aspx?id=21941&lib=law; *Notice on the Supervision of the Ride-Hailing Industry*, issued and effective on February 7, 2022, art. 5(2), http://lawinfochina.com/display.aspx?id=37711&lib=law&SearchKeyword=&SearchCKeyword=; *Draft Notice on Regulating the Business Operation in the Cloud Services*, issued on November 24, 2016, para. 9 (when providing services to users within China, cloud service providers must use servers in China and place the data processed in its territory), https://www.miit.gov.cn/gzcy/yjzj/art/2020/art_30d60a39446048edad54fd82075fb90f.html.
[1737] Cai, *supra* (*Jurisdictional Report*), 72.

sanctions imposed by such rules, sparse enforcement actions, and the absence of a centralized regulatory authority dedicated to governing cross-border data transfers.[1738]

B. Legislations and Regulations From 2017 to Present

(A) Cybersecurity Law

The tide was turning since the enactment of the *Cybersecurity Law* (CSL) in November 2016 (which became effect in June 2017).[1739] Exemplifying Chinese legislative efforts to centralize the previously piecemeal regulatory interventions, this law constitutes the cornerstone of a new, comprehensive data governance regime striving to secure China's digital sphere and implement security-oriented policies.[1740] Substantively, this omnibus legislation encompasses elements of online content control, critical infrastructure protection, personal information protection, and network operators' security obligations.[1741] Under the section titled "operation security of critical information infrastructures", article 37—for the first time—imposes horizontal requirements of data localization across all economic sectors.[1742]

As stipulated by this provision, "personal information" and "important data" collected and generated by critical information infrastructure (CII) operators must be stored within China's territory.[1743] As an exception, a transfer of such data outside China is possible only when it is necessary for the operators' business purposes, and must pass security assessments in accordance with relevant authorities' requirements.[1744] While establishing data localization requirements and cross-border data transfer restrictions, this provision only imposes such obligations on CII operators, as opposed to all "network operators".[1745] Due to their crucial role for a country's economic security and social stability, CII receives prioritized protection under this law,[1746] and thus, is subject to more stringent security obligations, including those on data storage and export.[1747]

Under the CSL, the notion of "CII" refers to network facilities and information systems that provide network information services to important industries and sectors, including public communication and information services, energies, transportation, water facilities, finance, public

---

[1738] *Id.*, 72-73 (noting that "before the Cybersecurity Law…. [t]he absence of a centralized authority leaves regulatory loopholes in practice, since industrial regulators only have jurisdiction over cross-border data transfers by entities in their industries and cannot effectively extend their jurisdiction to other ordinary enterprises transferring he same data").
[1739] Cybersecurity Law of the PRC, enacted on November 7, 2016, effective on June 1, 2017, http://www.lawinfochina.com/display.aspx?lib=law&id=22826 [CSL].
[1740] Creemers, *supra* (Emerging), 3-4.
[1741] *Id.*, 4; Qi et al., *supra*, 1346-51.
[1742] Cybersecurity Law, art. 37.
[1743] *Id.*
[1744] *Id.*
[1745] Under this law, "network operators" refer to the owners and managers of the network as well as network service providers. See art. 76(3), Cybersecurity Law.
[1746] *Id.*, art. 31.
[1747] Qi et al., *supra*, 1350.

services, e-government, national defence industry, and other important industries and sectors.[1748] If suffering damage, loss of function, or data breaches, CII may seriously endanger national security, national economy, people's livelihood, or public interests.[1749] While the specific lists of CIIs are to be made by relevant industrial or regional regulators, the identification of CII shall largely depend on (i) the importance of its network facilities and information systems to core business operations in the relevant industry or sector, (ii) the degree of damage generated, once the CII suffers damages or breaches, and (iii) the relevant implications for other industries and sectors.[1750] Under such a broad definition and relatively loose criteria of identification, CIIs may encompass a large amount of major ICT infrastructures and influential commercial networks commonly used by average people,[1751] provided that regulatory authorities perceive significant risks to national security or public interests.

In a similar vein, "important data" is vaguely defined as "data that—if altered, destroyed, leaked, breached, or illegally obtained or used—may directly affect national security, economic operations, social stability, or public health and safety."[1752] Identification of "important data" hinges on the interests the data may implicate, rather than who holds such data.[1753] Thus, personal information controlled by private-sector data controllers may also constitute important data, if, for example, those data involve huge numbers of data subjects in a sensitive sector.[1754]

Not surprisingly, the CSL's article 37 triggered much controversy in the international business community. During the legislative process, more than forty foreign business interest groups—led by American Chamber of Commerce—submitted a letter to challenge the enactment of such requirements, crying out fears that international business operations reliant on data stored in China may be severely undermined by the law, creating an unlevel playing field disfavoring foreign businesses.[1755] Despite such external pressures, the protest was unsuccessful, as China proceeded to finalize this rule without much change.[1756]

(B) Personal Information Protection Law

[1748] Cybersecurity Law, art. 31. State Council, *Regulation on Protecting the Security of Critical Information Infrastructure*, issued on July 30, 2021, effective on September 1, 2021, art. 2, http://www.lawinfochina.com/display.aspx?id=36511&lib=law [CII Protection Regulation].
[1749] Cybersecurity Law, art. 31; CII Protection Regulation, art. 2.
[1750] CII Protection Regulation, art. 9.
[1751] Qi et al., *supra*, 1350.
[1752] Cyberspace Administration of China (CAC), *Measures on Security Assessments for Cross-Border Data Transfers*, issued on July 7, 2022, effective on September 1, 2022, art. 19, https://www.lawinfochina.com/display.aspx?id=39000&lib=law [Security Assessment Measures].
[1753] Hong, *supra* note (Data Exit) ("determining what constitutes 'important data' requires us to stop judging by who holds the data and instead proceed by determining what values and interests the data can affect.").
[1754] *Several Provisions on the Management of Automobile Data Security (for Trial Implementation)*, issued on August 16, 2021, effective on October 1, 2021, art. 3 (providing that important data in the automotive sector includes personal data involving more than 100,000 data subjects), http://www.lawinfochina.com/display.aspx?id=36558&lib=law [Automobile Regulation].
[1755] *China Adopts Cybersecurity Law Despite Foreign Opposition*, BLOOMBERG (November 7, 2016), https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition#xj4y7vzkg.
[1756] Qi et al., *supra*, 1353.

After the CSL, as the perceived importance of data in economic, social, and governmental processes continued to grow, Chinese authorities increasingly shifted their regulatory focus towards scrutinizing private tech giants' data processing activities and data-driven business models.[1757] Within the central government, there was strong momentum for a more integrated approach to regulating the digital economy, which would *proactively* shape, rather than *reactively* respond to, the practices of prevalent online business models.[1758] In this context, the *Personal Information Protection Law* (PIPL) was adopted in August 2021,[1759] bearing the hallmark of these trends.[1760] Notably, it establishes a comprehensive legislative framework of personal data protection to regulate the relationship between data controllers and individuals whose data are collected and processed ("data subjects").[1761] But different from the EU's regulatory approach that creates fundamental rights applicable to both private and public sectors, the PIPL regulates the data processing activities of private and public actors separately, focused on the horizontal relationship between digital firms and data subjects.[1762]

Representing an incremental evolution of the CSL's framework, the PIPL incorporates a pre-existing set of personal data protection standards, but spells them out in greater detail, and extends them to a broader scope of application.[1763] Likewise, this legislation expands and develops the CSL's data localization requirements. Beyond CII operators, the PIPL extends the rule of data localization to every data-handling business ("data controller")[1764] that triggers the quantitative thresholds (as prescribed by the CAC), and to all governmental bodies.[1765] By virtue of this provision, these actors must locally store personal information collected and processed in China, unless passing a CAC-organized security assessment.[1766]

Relatedly, the PIPL stipulates both specific and general regulatory requirements for cross-border transfers of personal information. Specifically, article 38 of the law establishes three mechanisms for data controllers to transfer personal data outside China—security assessments, certification,

---

[1757] Creemers, *supra* (Emerging), 5 (describing "a shift in regulatory focus" post the CSL: while Chinese regulators' personal data protection efforts "had hitherto largely addressed malicious activities such as data theft, the business models, and practices of Chinas tech giants now came under growing scrutiny").
[1758] *Id.*, 6.
[1759] Personal Information Protection Law, issued on August 20, 2021, effective on November 1, 2021, https://www.lawinfochina.com/display.aspx?lib=law&id=36358 ["PIPL"].
[1760] Creemers, *supra* (Emerging), 6.
[1761] *Id.*, 2.
[1762] *Id.*, 8 (noting that the PIPL does not emulate the European fundamental rights to data protection and privacy, and it "largely leaves the power of government bodies untouched, as it does not impose meaningful constraints on their ability to collect and process data"). That said, the PIPL also contains five provisions to regulate Chinese governmental actors' collection and processing of personal data (the vertical relationship). But they are drafted in a general way, while permitting broad exceptions for purposes of fulfillment of statutory duties and responsibilities of public-sector actors. See PIPL, arts. 33-37.
[1763] Creemers, *supra* (Emerging), 6 (noting that while the CSL's data protection provisions only cover "network operators" and "CII" operators, the PIPL applies to "data controllers", including corporate and governmental actors).
[1764] "Data controllers" (referred to as "personal information handlers" by the PIPL in Chinese) are the organizations and individuals that can independently determine the purpose and means of the processing of personal data. The "processing" of personal data includes the collection, storage, use, transmission, provision, disclosure, and deletion of the data. See PIPL, arts., 4(2), 73(1).
[1765] PIPL, arts. 36, 40.
[1766] *Id.*, art. 40.

and standard contractual agreements.[1767] As noted, data controllers reaching the prescribed volume thresholds and governmental actors must file for security assessments before the CAC, in order to obtain the approval for transferring personal data outside China.[1768] Where the thresholds for security assessments are not triggered, a non-CII data controller may export personal information, if it (i) obtains certification from an accredited agency in accordance with CAC-approved standards, (ii) concludes a standard contractual agreement formulated by the CAC with a foreign recipient party, or (iii) passes the security assessments.[1769] When the PIPL was adopted, the CAC had not elaborated on the volume thresholds; nor had it specified regulatory requirements for certification or a standard contractual agreement.

In addition to satisfying the conditions specific to a selected transfer mechanism, data controllers must also fulfill three general sets of regulatory requirements prior to transferring personal data outside China.

First, they must adopt necessary measures to ensure that overseas data recipients' data processing activities satisfy the level of personal data protection provided by the PIPL.[1770] Second, data controllers are obliged to notify data subjects of the specifics about the transfer, and shall obtain their separate consent.[1771] Third, they must also conduct personal data protection impact assessments prior to data transfers.[1772] The impact assessments should evaluate the legality, propriety, and necessity of the transfers, as well as whether the measures adopted are legitimate, valid, and proportionate in relation to the degree of risks imposed; and the controllers must keep the reports and records for at least three years.[1773] As will be detailed later, these obligations seem to impose relatively onerous conditions for companies to fulfill, adding to their administrative burdens and compliance costs for cross-border data transfers.[1774]

Further, the PIPL's rules not only apply to data handling firms established in China, but also may reach foreign-based companies whose data processing activities occur outside China. Manifesting significant extraterritorial effects, this law applies to foreign data processing activities, where the purpose is (i) to provide products or services to natural persons in China; or (ii) to analyze the activities of natural persons in China.[1775] Foreign-based data controllers falling into this scope are required to designate a specific agency or representative to be responsible for handling personal data protection issues.[1776]

Together with their China-based agencies or representatives, such foreign companies are obliged to comply with Chinese regulations on data localization and cross-border data transfers. Specifically, where foreign data controllers directly collect personal data from individuals located

[1767] *Id.*, art. 38(1)(a)-(c).
[1768] *Id.*, arts. 36, 40
[1769] *Id.*, art. 38(1)(a)-(c).
[1770] *Id.*, art. 38(3).
[1771] *Id.*, art. 39.
[1772] *Id.*, art. 55.
[1773] *Id.*, art. 56.
[1774] See *infra* section V.A.(C).
[1775] PIPL, art. 3(2).
[1776] *Id.*, art. 53 (foreign data controllers should provide the contact information of their China-based agency or representative to the relevant authorities).

in China, they shall have their domestic agencies file for security assessments, if such data reach the CAC's prescribed volume thresholds.[1777] When the thresholds are not triggered, they should file for certification through their domestic agencies, or enter into standard contractual agreements with the latter, in order to make their data processing activities lawful under the PIPL.[1778]

As for cross-border transfers of personal data stored in China for law enforcement and judicial assistance purposes, the PIPL heavily restricts this possibility, in that it prohibits all data controllers to do so without the approval of Chinese supervisory authorities.[1779] As noted earlier, this provision seeks to ensure China's exclusive territorial jurisdiction over domestic data, safeguarding its data sovereignty against the extraterritorial reach of a foreign law (e.g., the U.S. CLOUD Act).[1780]

Finally, the PIPL contains two tripwire provisions with respect to cross-border personal data transfers, targeted at foreign private and governmental actors.[1781] First, the CAC may blacklist foreign organizations and individuals to limit or prohibit transfers of personal data to such recipients, where their data processing activities infringe on Chinese citizens' personal data or undermine China's national security or public interests.[1782] Second, the law authorizes Chinese authorities to adopt countermeasures against foreign governments that impose discriminatory prohibitions or restrictions against China with respect to personal information protection.[1783]

While it remains to be further clarified, this latter provision may cover the scenario where a foreign government targets Chinese digital platforms or ICT firms operating in its market for discriminatory motives (as perceived by China), and adopts restrictive measures hurting overseas Chinese investments and businesses. In this regard, illustrative examples include the U.S.'s restrictions on Huawei and ZTE, its divesture measures against TikTok, and the "Clean Network" program, all of which cited national security threats arising from the CCP's potential access to sensitive American data and its capacity to surveil U.S. actors through Chinese digital firms.[1784]

[1777] *Data Export FAQs (1): Whether Overseas Data Controllers under Article 3(2) of the PIPL Are Required to File for Security Assessments?*, TMT LEGAL FORUM (October 20, 2022), https://mp.weixin.qq.com/s/UiUTHjLH_z2ab8SQlNuyOw.

[1778] *China Unveils Draft Standard Contract and Provides Clarifications on Cross-Border Data Transfer Mechanisms*, LATHAM & WATKINS CLIENT ALERT COMMENTARY (August 9, 2022), at 7, https://www.lw.com/en/offices/admin/upload/SiteAttachments/Alert%202984.pdf ['China Unveils'].

[1779] PIPL, art. 41.

[1780] See *supra* section I.C.

[1781] Creemers, *supra* (Emerging), 6.

[1782] PIPL, art. 42.

[1783] *Id.*, art. 43.

[1784] See Diane Bartz & Alexandra Alper, *U.S. Bans New Huawei, ZTE Equipment Sales, Citing National Security Risk*, REUTERS (December 1, 2022), https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/ (noting the U.S. banned the sale or import of new Chinese telecommunication and surveillance equipment made by Huawei, ZTE, Hikvision, Dahua, and other Chinese companies, arguing that such equipment would create national security risks to the U.S.); Gavin Bade, *TikTok National-Security Deal Roiled by Internal Strife*, POLITICO (December 16, 2022), https://www.reuters.com/business/media-telecom/us-fcc-bans-equipment-sales-imports-zte-huawei-over-national-security-risk-2022-11-25/ (noting that the Biden administration is at odds over whether to compel ByteDance, the Chinese parent company, to divest from TikTok's U.S. operations, since the CCP may use the app and the U.S. data it collected to surveil Americans and the U.S. government, imposing a national security threat); U.S. Department of State, *The Clean Network*, https://2017-2021.state.gov/the-clean-network/index.html (noting that in August 2019,

According to PRC authorities, such allegations are groundless accusations abusing the concept of "national security", and are politically motivated to discriminate against Chinese companies for thinly veiled protectionist purposes.[1785] Together, these two provisions reflect the growing tensions between China and Western countries with respect to cross-border data flows in the digital realm.[1786]

(C) Data Security Law

Alongside the legislative process of the PIPL, China also formulated the *Data Security Law* (DSL), which entered into force in September 2021.[1787] Different from the PIPL that focuses on protecting data subjects vis-à-vis digital companies, the DSL's mandate is primarily to safeguard national security and public interests against potential risks arising from data stored in China, aimed at balancing competing goals of development and national security.[1788] For that purpose, this law creates a comprehensive, security-oriented regulatory framework to govern the processing activities of all data (whether personal or not, digital or in physical forms) by private and public actors, and to assess and manage the potential risks to such data—particularly against hostile forces inimical to China's regime security and national security at home and abroad.[1789]

As noted earlier, the DSL seeks to establish a "categorized and layered" data protection system as an overarching regulatory architecture.[1790] This system is designed to provide differentiated levels of protection to sensitive or important Chinese data, based on their relative importance for economic and social development, as well as the damage incurred to national security, public interests, and interests of individuals and organizations if breached, disclosed, or misused.[1791] Under this system, the DSL mandates local governments and industrial regulators to classify and catalogue "important data" in their regions and sectors, respectively, and requires them provide prioritized protection for those data.[1792] Further, the DSL creates a new category of data at the top level of national data protection system—"national core data" (i.e., the data that concern "national security, the lifelines of national economy, important aspects of people's livelihoods, exceptional public interests, etc.")—which are subject to more stringent regulatory standards than "important

---

Secretary of State Michael Pompeo launched the "Clean Network" program, which aimed to exclude untrusted and malign tech suppliers (e.g., Chinese firms) from U.S. Internet and ICT infrastructure, and which called for other like-minded countries to join the initiative).

[1785] Ministry of Foreign Affairs, *Reality Check: Falsehoods in US Perceptions of China*, June 19, 2022, https://www.mfa.gov.cn/eng/wjbxw/202206/t20220619_10706059.html.

[1786] Creemers, *supra* (Emerging), 6.

[1787] Data Security Law, issued on June 10, 2021, effective on September 1, 2021, https://www.lawinfochina.com/display.aspx?id=35666&lib=law&EncodingName=big5 ["DSL"].

[1788] Creemers, *supra* (Emerging), 6-7. See DSL, art. 1 (the enactment of this law is to regulate data processing activities, *safeguard data security, promote the exploitation and utilization of data*, protect individual and organizations' legal rights and interests, *safeguard national sovereignty, national security, and development interests*) (emphasis added).

[1789] Creemers, *supra* (Emerging), 2 (noting that the DSL "focused on creating a comprehensive architecture to assess and manage the potential risk emanating from every single piece of data held in China" from the view of national security and public interests). See DSL, arts. 2, 3. Data processing activities concerning state secrets and military data are excluded from the scope of the DSL. See *id.*, arts. 53, 54.

[1790] DSL, art. 21(1). See *supra* section I.C.

[1791] *Id.*

[1792] *Id.*, art. 21(1), (3).

data".[1793] To identify "important data" and "national core data", the focus should be the interests those data implicate, rather than who holds such data: in other words, large amounts of personal data held by a private-sector data controller may qualify as such, if the breach or misuse thereof can potentially endanger national security and public interests.[1794]

On this basis, the DSL requires Chinese regulators to establish three concrete risk management mechanisms to safeguard data security and national security. The first is a centralized set of mechanisms for data security risk assessment, reporting, information sharing, monitoring, and early warning, coordinating Chinese authorities' collection, evaluation, and analysis of information about such threats.[1795] Second, the government is mandated to set forth mechanisms to respond to data security emergencies, enabling Chinese regulators to execute emergency response plans and management measures to mitigate harms, address security concerns, and disclose relevant information to alert the public.[1796]

Third, the DSL mandates the establishment of the data security review mechanism, empowering regulatory authorities to examine domestic or extraterritorial data processing activities that impact or are likely to impact national security.[1797] Such decisions are final and binding, without a possibility of appeal.[1798] As will be detailed later, this provision offers a legislative basis for the CAC to implement and enforce cybersecurity review measures over Chinese digital firms handling large troves of personal data.[1799] In addition, the data security review mechanism may also apply to foreign investment transactions, where they may result in a foreign entity controlling or accessing important data or large amounts of personal information from China.[1800]

Finally, with respect to international business relationship, the DSL contains two specific provisions. First, it incorporates the substance of the PIPL's anti-sanction clause. Under article 26, the DSL authorizes Chinese authorities to adopt countermeasures against a foreign government, where the latter implements discriminatory prohibitions or restrictions against China in areas of trade and investment relating to data and digital technologies.[1801] Second, the DSL mandates the government to adopt export control measures for data related to protecting national security and national interests (or fulfilling international obligations).[1802] How this latter provision would be implemented by the authorities remains to be seen, but it may create more stringent conditions for the export of certain categories of important data implicating sensitive national security interests, requiring those data transfers to pass the scrutiny of China's *Export Control Law*.[1803]

[1793] *Id.*, art. 21(2).
[1794] Hong, *supra* note (Data Exit) ("determining what constitutes 'important data' requires us to stop judging by who holds the data and instead proceed by determining what values and interests the data can affect.").
[1795] DSL, art. 22.
[1796] *Id.*, art. 23.
[1797] *Id.*, art. 24(1), art. 2.
[1798] *Id.*, art. 24(2).
[1799] See *infra* sections V.C, and V.D.
[1800] See National Security Law, promulgated and effective on July 1, 2015, art. 59 (China establishes the national security review mechanisms over foreign investment activities, among others, that impact or are likely to impact national security), http://lawinfochina.com/display.aspx?id=19663&lib=law. The data security review mechanism under the DSL aims to implement and enforce such national security review mechanisms. See DSL, art. 24(1).
[1801] DSL, art. 26.
[1802] *Id.*, art. 27.
[1803] See e.g., Wu, *supra*, 83.

IV. REGULATORY INSTITUTIONS

In parallel to the salient trends to turn erstwhile sector-specific regulations to a comprehensive data governance framework, the powers of China's cyberspace regulatory institutions also have been centralized and consolidated in an overarching supervisory authority since the early 2010s. In this process, the newly created CAC rose to become a powerful ministerial-level super agency, mandated with unmatched regulatory authority and enforcement powers to regulate online content and data-related activities.

During the 2000s, China's Internet governance institutions were largely decentralized, with more than ten ministries and departments charged with relatively unclear duties.[1804] Unsurprisingly, such a multi-departmental governance model created not only unnecessary administrative burdens, but also overlapping and even competing jurisdictions between different authorities.[1805] This status quo started to change in May 2011, when the CAC was created to integrate and coordinate the previously fragmented Internet governance authorities.[1806] A ministerial-level agency, the newly established CAC was mandated with directing, coordinating, and supervising online content regulation and other duties of Internet governance.[1807] But at that time, the CAC was a subordinate department under the *State Council Information Office*,[1808] and its delegated authority to regulate the Internet was still incomplete.

In February 2014, China established the *Central Leading Group for Cybersecurity and Informatization* ("Leading Group") to formulate and implement national strategies of cybersecurity and informatization.[1809] Chaired by President Xi, the Leading Group enlisted many senior party leaders and high-profile officials as its members (including Premier Li, Keqiang acting as the deputy director).[1810] At the first meeting of the Leading Group, President Xi spelt out the foundation of China's "cyber superpower strategy", with its core being to integrate previously fragmented bureaucratic institutions and policy areas.[1811] Specifically, President Xi called for the Leading Group's centralized and unified leadership to advance national cybersecurity and

---

[1804] Liu, *supra* (*China's Data Localization*), 90.
[1805] *Id.*; Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 425-6 (describing the institutional problem of "Nine Dragon Tamed the Flood": the bureaucratic framework had created inefficient bureaucratic cooperation across ministries, partially overlapping competence of different authorities, and even turf battles among them).
[1806] *The General Office of the State Council Established the Cyberspace Administration of China, with Wang Chen Acting as the Director*, May 4, 2011, http://www.gov.cn/rsrm/2011-05/04/content_1857301.htm.
[1807] *Id.* (the CAC's other duties include handling administrative approvals of businesses related to online news reporting, directing the development of online gaming, online video, and online publication industries, promoting the construction of major news websites, managing government online publicity work, investigating and punishing websites violative of laws and regulations, overseeing telecom service providers in their management of domain name registration, IP address distribution, websites registration, and Internet access).
[1808] *Id.*
[1809] *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, *supra*.
[1810] Gao, *supra* (Data Regulation), 250-251 (noting that "[s]uch high-level set-up signals that cyber security and informatization have been elevated to an unprecedented level and have now become important components of the overall national security strategy"); Rogier Creemers, *China's Cyber Governance Institutions*, LEIDEN ASIA CENTRE REPORT (January 2021), at 5, https://leidenasiacentre.nl/report-chinas-cyber-governance-institutions/ ["Institutions"].
[1811] Creemers, *supra* (Institutions), 5. See *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, *supra*.

informatization strategies, positioning this entity at the top-level of China's cyberspace governance institutions.[1812] Though an *ad hoc* body then, the Leading Group had its office housed in the restructured CAC, which substantially elevated the latter's status and authority among its peer ministries and departments as it was under the direct leadership of President Xi.[1813]

In August 2014, the State Council delegated the CAC with the powers to lead national online content regulation, as well as the supervisory authority over law enforcement actions thereof.[1814] Such reinforced powers and authority effectively made the CAC the most powerful governmental agency to regulate the Internet in China.[1815] At the behest of President Xi, it is the CAC, a super ministerial-level regulatory authority, that primarily oversees cyberspace activities and executes the policies of the Leading Group.[1816]

In 2018, the Leading Group was reconfigured as a standing institutional body—the *Central Cybersecurity and Informatization Commission* ("Central Commission")—further strengthening its centralized authority, powers, and resources over cybersecurity and Internet governance.[1817] Focused on cybersecurity and informatization, most of the Central Commission's work concerns top-level digital policy-making, political leadership, interagency coordination, and settling interdepartmental tensions.[1818] But under the arrangement of "one body, two plaques", it is the CAC that houses the Central Commission and provides administrative support for most of its operations. [1819] Meanwhile, both the CAC and the Central Commission were elevated to independent agencies that directly answered to the Central Committee of the CCP.[1820] Thus, this reorganization further improves the CAC's institutional status and policymaking authority, while entrenching the CCP's capacity to supervise, monitor, and regulate China's cyberspace.[1821]

These institutional dynamics have witnessed the rise of the CAC as an overarching regulatory authority of Internet governance with concentrated regulatory powers over cyberspace. On top of

---

[1812] Creemers, *supra* (Institutions), 5. See *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, *supra*.
[1813] Gao, *supra* (Data Regulation), 251. See *State Internet Information Office Is Restructured, and the State Council Delegated It with the Powers on Internet Content Regulation and Enforcement*, GUANCHA (August 28, 2014), https://www.guancha.cn/politics/2014_08_28_261572.shtml.
[1814] *The Notice Concerning the State Council Delegating the Cyberspace Administration of China with the Mandate to Lead Online Content Regulation*, Guo Fa [2014] No. 33, August 28, 2014, http://www.gov.cn/zhengce/content/2014-08/28/content_9056.htm.
[1815] Gao, *supra* (Data Regulation), 251.
[1816] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 433.
[1817] Rogier Creemers et al., *China's Cyberspace Authorities Set to Gain Clout in Reorganization*, NEW AMERICA (March 26, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/ (noting that the Leading Group that typically addressed "a pressing shorter-term issues" was turned into a well-resourced Leading Commission "designed to provide a permanent bureaucratic solution) ["Reorganization"].
[1818] Creemers, *supra* (Institutions), 6. See *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, *supra*.
[1819] Creemers, *supra* (Institutions), 6, 8 (noting that "as the main working body of the (Commission, the CAC) plays a major coordinating role in the organization of digital policy.").
[1820] *The Notice Concerning the Newly Restructured Institutions of the State Council*, Guo Fa [2018] No. 6, March 24, 2018, http://www.gov.cn/zhengce/content/2018-03/24/content_5277121.htm.
[1821] Creemers et al, *supra* (Reorganization) (noting that this change "inject(s) the Party more directly into managing key sectors (of cyberspace)").

that, the CSL, DSL, and PIPL have further consolidated the CAC's authority and competence to regulate cybersecurity, personal information protection, and cross-border data transfers.

In 2016, the CSL strengthened the authority of the CAC as a super agency to supervise and coordinate regulatory activities of regional and sector-specific authorities on cybersecurity protection.[1822] Meanwhile, it appointed the CAC as a centralized authority for national CII regulation, and mandated it to enact and enforce regulatory standards of security assessments for CII operators' cross-border data transfers.[1823] Likewise, the DSL authorized the CAC to establish regulatory requirements for non-CII data controllers to transfer important data outside China.[1824]

In 2021, the PIPL designates the CAC as a centralized agency to oversee and coordinate national personal information protection initiatives,[1825] without creating independent, specialized data protection authorities. With respect to cross-border personal data transfers, this law appoints the CAC to formulate and implement specific regulatory standards for three mechanisms of data export—security assessments, certification, and standard contractual agreements.[1826]

In short, the CSL, DSL, and PIPL empower the CAC to steer the promulgation and implementation of ancillary regulations to concretize the basic regulatory framework set by such laws at a high-level. These legislative mandates ushered in a set of implementing regulations that provided detailed procedures, obligations, and prescriptive requirements for cross-border data transfers and data processing activities, which will be canvassed in the next Part.

Finally, the CSL, PIPL, and DSL have also vested the CAC with robust law enforcement authority to enforce their rules. Under these laws, the CAC is authorized to impose heavy sanctions against data operators for their non-compliance with cybersecurity and data protection obligations, including data localization and cross-border transfer requirements.[1827] To correct such breaches, the CAC may order a data-handling business to rectify its non-compliance activities, confiscate its illegal proceeds, and suspend or terminate its provision of services or products.[1828] Under the most extreme scenario, the company may face administrative fines of up to 50 million yuan or 5% of their annual gross revenue of the preceding year (whichever is higher), suspension or termination of business operations, and revocation of business licenses.[1829] With substantial delegated power resources as such, the CAC can deploy hefty sanctions to ensure compliance and deter breaches, playing a prominent monitoring role to protect cybersecurity and national data security.

V. IMPLEMENTING REGULATIONS

From 2017 onwards, the CAC has been promulgating a flurry of regulatory standards to implement the legislative framework established by the CSL, PIPL, and DSL, with a focus on cross-border

[1822] CSL, arts. 8, 39, 51.
[1823] *Id.*, arts. 35, 37, 39.
[1824] DSL, art. 31.
[1825] PIPL, arts. 60, 62.
[1826] *Id.*, arts. 38, 40.
[1827] See eg., CSL, art. 66; PIPL, art. 66; DSL, arts. 46, 48.
[1828] See eg., CSL, art. 66; PIPL, art. 66; DSL, arts. 46, 48.
[1829] PIPL, art. 66.

data transfers. The sections below identify and summarize four salient themes. The first is concretizing the prescriptive requirements of three cross-border data transfer mechanisms. The second is adopting new sector-specific regulations to impose stricter standards for sensitive industries. The third is developing the cybersecurity review mechanism to scrutinize data processing activities implicating national security threats. The fourth is formulating a comprehensive regulation to implement and develop the regulatory standards set forth by the CSL, PIPL, and DSL.

A. Concretizing Three Mechanisms of Cross-Border Data Transfers

(A) Security Assessments as the Safety Valve of Cross-Border Data Transfers

While security assessments are designed to play a central role in facilitating cross-border data transfers from China, the concrete regulatory standards went through a pronged rule-making process, whereby the authorities recalibrated policy solutions to respond to business interest groups' concerns and balance competing interests. Before its adoption of the *Measures on Security Assessments for Cross-Border Data Transfers* ("*Security Assessment Measures*") in July 2022,[1830] the CAC already has released three different versions of draft measures in 2017, 2019, and 2021, respectively.

In April 2017, the CAC published the first draft regulation on security assessments to implement the CSL's provision on cross-border data transfers for CII operators.[1831] Notably, unlike the CSL that imposed data localization requirements merely on CII operators, this regulation went substantially further: it extended this rule to every network operator handling personal information and important data in China, requiring them to store all of such data domestically.[1832] Under this rule, all personal information and important data collected and generated in China must pass security assessments for outbound transfers.[1833] Not surprisingly, such a change triggered outcry from the international business community and China's major trading partners. For instance, the U.S. filed a submission to the Council for Trade in Services of the World Trade Organization (WTO), expressing concerns that China's CSL and draft measures may violate its commitments under the General Agreement on Trade in Services.[1834] In addition, the draft measures also met with significant backlash from Chinese digital industry, particularly national tech champions

[1830] See Security Assessment Measures, *supra*.
[1831] CAC, *Draft Measures on Security Assessments for Cross-Border Transfers of Personal Data and Important Data*, April 11, 2017, http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. See CSL, art. 37.
[1832] *Id.*, art. 2.
[1833] *Id.*
[1834] *Communication from the United States—Measures Adopted and under Development by China Relating to Its Cybersecurity Law* [2017 U.S. WTO Submission], September 26, 2017, S/C/W/374, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf&Open=True (arguing that "China's measures would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business… the measures would impose special scrutiny, particular procedures, or bans on the cross-border transfer of expansive and loosely-defined categories of data. The result would be to discourage cross-border data transfers and to promote domestic processing and storage. The impact of the measures would fall disproportionately on foreign service suppliers operating in China….").

seeking global markets.[1835] This is because unduly burdensome cross-border data transfer requirements would severely increase their compliance costs and undermine their development of cloud services, AI-related technologies, and consumer-tracking products around the world, in the same ways that such rules would adversely impact foreign companies.[1836] Given the international and domestic backlash, the CAC eventually dropped such draft measures.[1837]

Two years later, the CAC issued another draft regulation on security assessments for cross-border transfers of personal data in June 2019.[1838] Evincing the CAC's recalibrated policy response, this instrument deleted the controversial provision that expanded data localization requirements to all network operators.[1839] However, it still required all network operators to pass security assessments for exporting personal information and important data from China.[1840] Substantively, the 2019 version retained most of the 2017 draft's provisions, though it added clarifications on a few issues, such as the particulars to be reviewed during the CAC's security assessments, and that data exporters and recipients must conclude data transfer contracts.[1841] At the time, security assessments were designated as the only lawful data transfer mechanism, potentially subjecting all outbound data flows to Chinese authorities' *ex ante* regulatory approval. As were the 2017 draft measures, this proposed regulation was never adopted by the CAC, rendering the CSL's cross-border data transfer provision largely inoperable in practice.

After the PIPL was enacted, the CAC released a third draft regulation on security assessments in October 2021, which substantially revised its scope of application and specified more detailed requirements for outbound data transfers.[1842] Most of its provisions were incorporated into the final version of the 2022 Security Assessment Measures.[1843] Compared with its 2017 and 2019 predecessors, the finalized measures made important revisions and clarifications in the following major aspects.

First, it prescribes a set of thresholds for triggering the CAC's mandatory security assessments. As noted earlier, the CSL required CII operators who transfer important data and personal information to pass security assessments.[1844] In addition to reiterating this requirement, the regulation obliges all data controllers who transfer important data outside China to pass security assessments.[1845] Further, it provides that the thresholds for security assessment will also be triggered, where personal information is to be transferred by a data controller (i) who has processed personal information of more than 1 million individuals, or (ii) who has cumulatively transferred personal

[1835] Samm Sacks, Paul Triolo, and Graham Webster, *Beyond the Worst-Case Assumptions on China's Cybersecurity Law*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (October 13, 2017), https://www.csis.org/blogs/technology-policy-blog/beyond-worst-case-assumptions-chinas-cybersecurity-law.
[1836] *Id.*
[1837] Creemers, *supra* (Emerging), 5.
[1838] CAC, *Draft Measures on Security Assessments for Cross-Border Transfers of Personal Data*, June 13, 2019, http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.
[1839] *Id.*, art. 2.
[1840] *Id.*
[1841] *Id.*, art. 6, 11, 13-17, 20.
[1842] CAC, *Draft Measures on Security Assessments for Cross-Border Data Transfers*, October 29, 2021, http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm.
[1843] *Security Assessments Measures*, *supra*.
[1844] CSL, art. 37.
[1845] *Security Assessments Measures*, art. 4(1).

information of more than 100,000 individuals, or sensitive personal information of more than 10,000 individuals outside China since January 1 of the previous year.[1846] Unless passing CAC-organized security assessments, these data controllers must localize the storage of personal information within China.[1847] Such quantitative thresholds have considerably narrowed the applicability of security assessments compared with the 2017 and 2019 draft regulations. That said, in addition to these scenarios, the CAC may further prescribe other circumstances necessitating security assessments in new regulations.[1848]

Meanwhile, as clarified by the CAC's guidance, security assessments apply not only to outbound transfers of data collected and generated in China, but also to the provision of the rights to access and use China-stored data to foreign organizations or individuals (i.e., the grant of remote access to data).[1849] Under this broad interpretation, both scenarios constitute "cross-border data transfer activities" governed by this regulation, and thus, must pass security assessments.

Second, the regulation spells out fully-fledged requirements on how to apply security assessments. Under the regulation, data controllers are required to conduct a self-assessment to evaluate risk factors associated with the transfer, prior to applying for a formal security assessment from the CAC.[1850] These risk factors include (i) the legality, propriety, and necessity of the data transfers, and the purposes, scope, and means of the overseas recipients' data processing; (ii) the quantity, scope, categories, sensitivity, and risks of the data to be exported, (iii) the duties and obligations undertaken by overseas data recipients, as well as the latter's protection capabilities (i.e., whether its corporate governance system and technical measures are adequate to ensure data security); (iv) security risks during and after the data transfers, and the protection of personal data in the recipient jurisdiction; (v) whether the binding legal instruments concluded by data controllers and overseas recipients provide sufficient obligations to ensure data security.[1851] The reports of these assessments must be submitted to the CAC, among others, to initiative the security review process.[1852]

During the formal review process, the CAC would conduct a more comprehensive review to evaluate relevant risk factors, focused on potential risks imposed by the data transfers to national security, public interests, and private rights and interests.[1853] In addition to all the factors involved in the self-assessments, this assessment would also consider (i) the impact of local laws, regulations, policies, and cybersecurity environment of the recipient jurisdiction on protection of outbound data, and whether the recipient party's data protection standards achieve the level of protection provided by Chinese laws; (ii) whether data security and personal information

[1846] *Id.*, art. 4(2)-(3).
[1847] PIPL, art. 40. See Kevin Duan et al., *CAC Formally Promulgates the Assessment Measures for Data Export*, HAN KUN LEGAL COMMENTARY (July 19, 2022), https://www.mondaq.com/china/security/1216766/cac-formally-promulgates-the-assessment-measures-for-data-export (noting that this provision is to clarify and implement article 40 of the PIPL, which requires data controllers reaching CAC-prescribed thresholds to store personal data within China unless they pass security assessments to export such data).
[1848] *Security Assessments Measures*, art. 4(4).
[1849] CAC, *Guidance for Filing for Security Assessments for Outbound Data Transfers (First Edition)*, https://insights.nymity.com/assets/media/en/09715b4c-d3de-4da1-87bc-1055df49801a.pdf.
[1850] *Security Assessments Measures*, art. 5.
[1851] *Id.*
[1852] *Id.*, art. 6.
[1853] *Id.*, art. 8.

protection can be adequately safeguarded; and (iii) data controllers' and recipient parties' compliance with Chinese laws, regulations, and rules.[1854]

As such, the substantive elements under the CAC's security assessment review are much more expansive than the EU's "adequacy" assessments, which are based on the laws, institutions, and international commitments of a third country for personal data protection.[1855] In addition to the data protection level ensured by a recipient jurisdiction (focused by the EU), the CAC also examines the necessity of the data transfers,[1856] the recipient party's data protection standards and security measures, and the parties' contractual provisions on data protection. Under this Chinese approach, protection of individuals' data privacy is just part of the CAC's overall evaluation, and its scrutiny is focused on national security risks implicated in the transfers.[1857]

Procedurally, the security assessment starts with a preliminary review at the provincial CAC office (to examine whether the application materials are complete), and then may proceed to the CAC at the state level for a substantive review.[1858] In the assessment process, the CAC may obtain input from other regulatory authorities (including relevant departments of the State Council, provincial CAC offices, and specialized agencies) to assist it in rendering a decision.[1859] The whole process may take around three months to complete, and is subject to the CAC's discretionary extensions, without a limit for the entire timespan.[1860]

Third, the regulation reinforces the CAC's authority to continuously monitor and supervise its decisions on security assessments. In principle, if a data controller passes a security assessment, the validity of that decision will last for two years,[1861] during which period the company is allowed to conduct uninterrupted data transfer activities covered by the decision with the same recipient.[1862] However, the regulation requires a data controller to re-apply for a new security assessment, if there are any changes in risk factors evaluated in the original assessment, which may affect data security.[1863] These circumstances may include changes in (i) the purposes and means of the overseas recipients' data processing, (ii) the scope, categories, or retention periods of the exported data, (iii) the recipient jurisdiction's laws, regulations, and cybersecurity environment, (iv) the actual controllership of recipient parties, or (v) the legal instruments concluded between data controllers and recipients.[1864] And where the CAC finds any data transfer activity that already passed a security assessment no longer satisfies the security requirements in practice, it may order

---

[1854] *Id.*
[1855] See GDPR, art. 45.
[1856] Duan et al, *supra* (noting that the "necessity" is undefined under the regulation, and it is unclear whether a company's additional costs in operation and compliance incurred by data localization can contribute to "necessity" of data transfer as such).
[1857] Hong, *supra* (Data Exit) (arguing that "the Measures focus on security interests at the national and societal level and specifically seek to eliminate or contain risks related to transferring data abroad.")
[1858] *Security Assessments Measure*, art. 7.
[1859] *Id.*, art. 10.
[1860] *Id.*, arts. 7, 11, 12. If the CAC finds that the case is complicated or there are materials to be supplemented or corrected, it may extend the assessment for an appropriate period. But there is no explicit limit for this "appropriate period". See *id*., art. 12.
[1861] *Id.*, art. 14.
[1862] Duan et al., *supra*.
[1863] *Security Assessments Measure*, art. 14.
[1864] *Id.*

the controllers to suspend or terminate the data transfers.[1865] In such a case, data controllers shall adopt measures to rectify its non-compliance before applying for a new assessment.[1866]

As such, the CAC makes it clear that security assessments are by no means "one-and-done" decision-making, but rather "living" processes under Chinese regulators' continuous monitoring and supervision. When finding new circumstances that may cause data transfers to undermine China's cybersecurity, national security, or individuals' data privacy, the CAC is empowered to restrict or prohibit such transfers, unless the controllers adopt supplementary measures to effectively remedy the issues identified. By allowing the CAC to periodically check whether its past decisions are still factually and legally sound, this mandate significantly expands the scrutiny of its security assessments. Such powers may prove instrumental to adapting the security assessment processes to subsequent developments or changed circumstances (regarding data controllers, recipient parties, or a destination jurisdiction's laws and policies) that may potentially affect data security and national security.

(B) Alternative Mechanisms of Certification and Standard Contractual Agreements

Alongside the rulemaking process for security assessments, the CAC has also drafted regulatory standards for two alternative cross-border data transfer mechanisms—certification and standard contractual agreements.[1867] For data controllers that fall outside the CAC's prescribed thresholds for security assessments, they are eligible to resort to these two mechanisms to transfer personal data outside China.

Similar to the Binding Corporate Rules under the GDPR,[1868] the certification mechanism seeks to implement and enforce a uniform set of data processing rules for cross-border data transfers within multinational organizations.[1869] As required by the certification mechanism, data controllers (i.e., the data exporters) and overseas recipients (such as a foreign branch of the corporate group) must conclude binding and enforceable legal agreements to protect data subjects' information privacy

[1865] *Id.*, art. 17.
[1866] *Id.*
[1867] In December 2022, the National Information Security Standardization Technical Committee (TC260) (a national standard-setting body under the CAC) released the *Technical Specification on Certifications for Personal Data Cross-Border Processing Activities*, which provides guidance on how to implement the certification mechanism. In June 2022, the CAC issued the *Draft Provisions on Standard Contracts for Cross-Border Transfers of Personal Data* and the CAC-formulated *Template of Standard Contractual Agreements*. See TC260, *Technical Specification on Certifications for Personal Data Cross-Border Processing Activities*, December 2022, https://www.tc260.org.cn/front/postDetail.html?id=20221216161852 [Certification Specification]; CAC, *Provisions on Standard Contractual Agreements for Outbound Transfers of Personal Data*, promulgated on February 22, 2023, effective on June 1, 2023, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm [Standard Contractual Provisions].
[1868] See GDPR, art. 47.
[1869] Certification Specification, arts. 2, 5.1(f), 5.3. In addition, the certification mechanism may also be used by overseas data controllers whose processing activities are subject to the PIPL's extraterritorial reach. This means that foreign-based data controllers that directly collect personal data from individuals in China to analyze their behavior or for marketing purposes can resort to certification to export such data. In this case, the domestic agency or designed representative of the overseas data controllers should apply for certification and assume legal liability. See PIPL, art. 3(2); Certification Specification, art. 2. To clarify, the certification mechanism is of a voluntary nature, and the Chinese authorities encourage and recommend companies that fall into these two categories to apply for certification. See *id.*, art. 4(f).

for intra-group data transfers cross borders.[1870] Such instruments must grant data subjects individual rights provided under the PIPL, as well as the rights to bring complaints or legal actions to Chinese authorities.[1871] Meanwhile, the overseas recipients must undertake to comply with data processing rules that govern the data controllers, to ensure that the level of data protection is not lower than the standards under applicable PRC laws, to accept the supervision of Chinese certification agencies (e.g., to respond to their inquiries and investigations), and to comply with applicable PRC laws and accept their jurisdiction.[1872] In this way, both data exporters and overseas recipients are required to provide the level of protection ensured under PRC laws, and to subject themselves to Chinese regulators' supervision and jurisdiction.

On the other hand, the certification process imposes relatively burdensome compliance requirements. In terms of corporate governance, both a data controller and an overseas recipient must appoint its own data protection officer (DPO), and establish its respective data protection department, in order to ensure that personal data protection obligations are complied with.[1873] The DPO must have expertise in personal data protection and relevant management experience, and should be a senior management member of the organization.[1874] The data protection department is mandated to formulate and implement data processing rules, conduct personal data protection impact assessments, supervise cross-border personal data transfer activities, and handle data subjects' requests and complaints.[1875] This obligation goes further than the PIPL's requirements, which only oblige data controllers whose processing activities reach statutory thresholds to designate a DPO.[1876] In addition, data controllers must conduct data protection impact assessments prior to cross-border transfers.[1877]

Different from the certification mechanism that is designed to primarily serve intra-group data transfers within a group of enterprises, a standard contractual agreement is available for any data controllers[1878] not triggering the CAC's volume thresholds.[1879] Substantively, the CAC-formulated model contract stipulates the obligations and duties of data controllers and overseas recipients, the due diligence obligation of both parties to assess the impacts of the recipient jurisdiction's laws and policies on the fulfillment of the contract, individual rights of data subjects, remedies, terms of contract termination, liability for breach of contract, and dispute settlement

[1870] Certification Specification, art. 5.1.
[1871] *Id.*, art. 6.1.
[1872] *Id.*, arts. 5.1, 6.2. See *id.*, art. 5.3.
[1873] *Id.* arts. 5.2.1, 5.2.2.
[1874] *Id.*, art. 5.2.1.
[1875] *Id.*, art. 5.2.2.
[1876] PIPL, art. 52.
[1877] The factors to be assessed are similar to those evaluated in the self-assessments as provided under the Security Assessment Measures, though they are framed in less prescriptive ways. See Specification, art. 5.4; see also Security Assessment Measures, art. 5.
[1878] Different from the Standard Contractual Clauses under the GDPR, the Chinese standard contractual agreements do not distinguish between the roles of data exporters and importers as "controllers" or "processors". See Phoebe Yan et al., *China Enhances Scrutiny for Cross-Border Data Transfer that Would Impact Multinational Companies*, PAUL HASTINGS INSIGHTS (July 18, 2022), https://www.paulhastings.com/insights/client-alerts/china-enhances-scrutiny-for-cross-border-data-transfer-that-would-impact.
[1879] Standard Contractual Provisions, art. 4. The Standard Contractual Provisions explicitly provides that data controllers cannot circumvent the security assessments by segregating data volumes and transferring personal data that is bound to pass the former process through standard contractual agreements. *Id.*

clauses.[1880] The data controllers and recipient parties must strictly incorporate the clauses of the CAC's model contract in their own agreements, though they may stipulate additional provisions that are not in conflict with the former.[1881]

Procedurally, data controllers must file the standard contractual agreements and data protection impact assessment reports[1882] with the provincial CAC office, in order to fulfill the compliance requirements for using this mechanism to export personal data.[1883] And data controllers must complete new impact assessments, re-sign standard contractual agreements, and then fulfill the filing procedure again, where (i) there are significant changes to the data transfers or the data to be exported,[1884] or (ii) changes in the recipient jurisdiction's laws and policies may affect personal data protection.[1885]

While aimed at facilitating cross-border personal data transfers, these two mechanisms are subject to important constraints, which may limit their effectiveness in practice. Procedurally, they seem to impose relatively onerous regulatory requirements, potentially generating significant administrative burdens and compliance costs for companies to export data. For instance, the certification mechanism not only requires data controllers to designate their DPOs and establish their data protection departments, but also demands overseas recipients to do the same, which may make certification overly burdensome and expensive for companies exporting small amounts of personal data.[1886] And if data controllers want to use the CAC-formulated model standard contractual agreement to export personal data, they must complete the mandatory filing procedure with the CAC, which can create high administrative costs for companies whose business models require uninterrupted cross-border data flows.[1887] Further, in order to use both mechanisms, data controllers (and overseas recipients in the certification process) must inform data subjects of the particulars about the transfers, and then obtain their separate consent.[1888] This general requirement may prove burdensome for data-intensive firms whose daily operation involves processing large volumes of personal data.

More importantly, given the relatively low volume thresholds triggering mandatory security assessments, it is unclear how certification or standard contractual agreements can provide a long-term solution for continuous cross-border data flows. In other words, these two alternative mechanisms are largely designed to serve small-scale data controllers, and are most suitable for relatively short-term transfers that do not involve huge amounts of data.

[1880] See CAC, *Annex: Standard Contractual Agreement for Outbound Transfers of Personal Data*, February 22, 2023, http://www.cac.gov.cn/2023-02/24/c_1678884830036813.htm.
[1881] Standard Contractual Provisions, art. 6.
[1882] The factors to be evaluated in the assessments are substantially similar to those required for self-assessments in the mandatory security assessment processes. See *id.*, art. 5.
[1883] *Id.*, art. 7.
[1884] These circumstances include changes to the purposes and means of the transfers by the data controllers, changes to the scope, categories, sensitivity, and storage location of the data to be transferred, changes to the purposes and means of the recipient party's data processing activities, or extension in the overseas storage period. *Id.*, art. 8.
[1885] *Id.*, art. 8.
[1886] *China's Certification for Personal Information Export Underway?*, BIRD AND BIRD INSIGHTS (May 31, 2022), https://www.twobirds.com/en/insights/2022/china/chinas-certification-for-personal-information-export.
[1887] *China Unveils*, *supra*, 10. See Draft Standard Contract Provisions, art. 12 (providing that the failure to comply with the filing procedure may result in a breach of the PIPL, generating legal responsibilities).
[1888] Certification Specification, art. 6.2(a); PIPL, art. 39.

(C) "The Hard Way Out?"

In retrospect, these rules have fleshed out the long-awaited regulatory standards to govern outbound data transfers from China, imposing relatively stringent requirements for exporting data collected and generated within the PRC territory.

First, Chinese regulations have created broad and sweeping *de jure* requirements of data localization on data-handling businesses. Under the CSL, if a company falls under the relatively broad and ambiguous scope of "CII operators" (including Internet service providers and social media platforms),[1889] then it must store personal information and important data within China's territory.[1890] In addition, the PIPL further extends the data localization requirements to data controllers whose processing activities of personal information trigger the CAC's prescribed thresholds, characterized by relatively low volumes.[1891] For these actors, transfer of data outside China is only possible when necessary for their business purposes and must pass the CAC's security assessments.[1892] Given the default rules of localized storage for such data, the CAC may apply a stricter standard to assess the necessity of the transfer and/or the data security risks imposed by the transfer during the review process.

Second, since the mechanisms for cross-border data transfers are relatively onerous, exacting, and costly, foreign firms with data-intensive businesses may be forced to accept localized storage and processing of data as a default solution.[1893] In other words, under Chinese regulations, the restrictive regulatory standards for outbound data transfers may function as *de facto* data localization measures, leading foreign businesses to localize data storage by default.

For large-scale transfers of personal information or transfers of important data, data controllers have to apply for security assessments and obtain the CAC's authorization on an *ad hoc* basis. Substantively, Chinese authorities' security assessments scrutinize not only the level of data protection provided by a recipient country, but also the protective measures, commitments, and duties of the parties (including data exporters and importers).[1894] Given the CAC's expansive review in search for potential data security risks, the assessment process can be protracted, clandestine, and uncertain. Since the evaluation of key elements (such as data protection laws, policies, and cybersecurity environment of the recipient jurisdiction, the security risks of data in transit or after transfers)[1895] is often subject to Chinese authorities' discretionary judgments, implementation of the assessments may largely depend on the CAC's perceptions, understandings, and calculations of open-ended risk factors, resulting in a relative low level of legal predictability and certainty.

[1889] Erie and Streinz, *supra*, 31.
[1890] CSL, art. 37.
[1891] PIPL, art. 40; Security Assessment Measures, *supra*, art. 4(2)-(3).
[1892] CSL, art. 37; PIPL, art. 40.
[1893] Erie and Streinz, *supra*, 31-2.
[1894] Security Assessment Measures, *supra*, arts. 8-9.
[1895] *Id*.

While certification and standard contractual agreements can facilitate small-scale data controllers' short-term transfers of personal data below the statutory volumes, the corporate governance requirements (i.e., designating DPOs and establishing data protection departments) and mandatory filing procedure are relatively burdensome and costly, and can be challenging to fulfill in practice.[1896] Further, given that the CAC's volume thresholds are relatively easy to trigger, these two alternative mechanisms cannot provide a long-term solution for data-reliant firms' regular, routine and large-scale transfers of personal information.

In addition, to transfer personal data outside China (whether through a security assessment, certification, or a standard contractual agreement), a data controller must notify a data subject of the particulars about the transfer, and obtain her separate, informed consent for the data export.[1897] As part of the *ex ante* compliance requirements for all data exports, this procedural obligation might be seen as unusually onerous,[1898] given that obtaining a data subject's explicit consent can constitute an independent ground for an outbound data transfer even under the GDPR (which is widely known for its strict terms for data exports).[1899] To utilize each mechanism of cross-border personal data transfers, controllers also have to conduct personal data protection impact assessments, and keep the reports and records for at least three years.[1900] As noted earlier, for security assessments and standard contractual agreements, these impact assessment reports must also be filed with Chinese regulatory authorities.[1901] Together, these additional conditions may impose burdensome requirements for foreign firms to navigate before exporting personal data from China, generating high administrative costs and bureaucratic burdens to ensure compliance.

B. Sector-Specific Regulations: The Example of the Automobile Sector

In addition to implementing three mechanisms of cross-border data transfers, the CAC also has been driving the rulemaking of sectoral regulations to manage data processing in sensitive sectors. Along with other sector-specific regulators, the CAC has subjected data collection and transfers in these areas to strengthened regulatory scrutiny, with the automobile industry being a prominent example.

While the automotive sector has long been subject to China's restrictive regulations (especially on the market access condition), such rules have been mostly about protecting domestic infant industry from international competition in the past.[1902] But with the increasing proliferation of smart and connected vehicles in the street, China's automotive regulations drastically accelerated since around 2020, largely driven by prominent data security and national security concerns. As a background, it bears noting that in 2020, nearly half of the new vehicles sold in China are capable

---

[1896] Certification Specification, arts. 5.2.1, 5.2.2; Draft Standard Contract Provisions, art. 7.
[1897] PIPL, art. 39.
[1898] See e.g., 2017 U.S. WTO Submission, *supra*, para. 3(c) (describing the consent requirement as "an extraordinarily burdensome requirement that could disrupt business operations….").
[1899] GDPR, art. 49(1)(a).
[1900] PIPL, art. 56.
[1901] *Security Assessments Measure*, art. 6; Standard Contractual Provision, art. 7.
[1902] Justin Ling, *Is Your New Car A Threat to National Security?*, WIRED (July 1, 2022), https://www.wired.com/story/china-cars-surveillance-national-security/ (noting that "[u]ntil 2021, foreign automakers had to find a Chinese partner in order to open shop in the country") ["*New Car*"].

of connecting to the Internet.[1903] Packed with built-in cameras, sensors and radars, these smart cars typically are able to constantly capture and record images of the surrounding environment, collect data about when, how, and where these vehicles are being used, and store those data in cloud-based servers.[1904] This means that the manufacturers can amass large troves of data about the drivers, passengers, vehicles, pedestrians, and surroundings.[1905] While much of such data may be necessary for a vehicle to properly function, the substantial data collection and sharing capacities of smart cars indeed raise strong security concerns for the PRC government.[1906]

In response, Chinese authorities have been tightening domestic regulations on smart cars, initially targeting U.S. electric carmaker Tesla—one of the most popular electric vehicles in China and perhaps the most connected one among new-generation automobiles.[1907] In March 2021, unpublished notices of the government allegedly prohibited Tesla from entering Chinese military complexes and restricted its use by military staff and employees of key state-owned enterprises, citing security concerns over cameras installed on its vehicles.[1908] And there were reported incidents of Tesla cars being banned from Chinese cities during high-level government meetings on an *ad hoc* basis.[1909] Following Tesla's recall of its electric vehicles sold in China due to a potential safety hazard, the CAC, along with four other ministries of the State Council, jointly issued a set of rules to regulate data processing activities in the automotive industry in August 2021.[1910] As the first sector-specific regulation to implement the CSL, DSL, and PIPL, this instrument represents a regulatory response to the government's growing security concerns arising from smart vehicles' immense surveillance potential.[1911]

[1903] Dashveenjit Kaur, *China Tightens Smart Vehicle Data Regulation for Tesla and Others*, TECH WIRE (August 26, 2021), https://techwireasia.com/2021/08/china-tightens-smart-vehicle-data-regulation-for-tesla-and-others/ (noting that this means that "the driver can open the window, adjust the inside temperature or play music or videos using voice recognition technology through the internet"); *China Steps Up Automobile Data Protection*, CHINA DAILY (August 21, 2021), http://english.www.gov.cn/statecouncil/ministries/202108/21/content_WS612033f6c6d0df57f98deeaf.html (noting that "the Ministry of Industry and Information Technology said around 15 percent of vehicles sold in the country last year had some form of autonomous functions. That means over 3 million vehicles with cameras or radar hit Chinese roads in 2020.").

[1904] Keith Zhai and Yoko Kubota, *China to Restrict Tesla Use by Military and State Employees*, WALL STREET JOURNAL (March 19, 2021), https://www.wsj.com/articles/china-to-restrict-tesla-usage-by-military-and-state-personnel-11616155643.

[1905] Ling, *supra* (*New Car*).

[1906] *Id.* (noting that "even if anonymized, general data being relayed from a fleet of Chinese-made cars in North America could reveal individual patterns and habits but also paint a complex picture of an entire neighborhood or city—be it the daily routine of an urban military base or the schedule of a powerful cabinet minister.").

[1907] *Id.*; *Tesla Cars Banned from China's Military Complexes on Security Concerns—Sources*, REUTERS (March 19, 2021), https://www.reuters.com/article/us-tesla-china-idUSKBN2BB18R (noting that Tesla built its first overseas factory in Shanghai in 2019, and its Model 3 sedans once were the best-selling electric vehicle in China).

[1908] *Tesla Cars Banned*, *supra*; Zhai and Kubota, *supra.*

[1909] Ling, *supra* (*New Car*) (noting that Tesla cars "are strictly banned on the streets of (Beidaihe) for the next two months, as senior Communist leadership descends on the city for a secret conclave", and that previously, "Chengdu barred Teslas in advance of a June visit from President Xi Jinping.").

[1910] Automobile Regulation, *supra*. This regulation was effective on October 1, 2021. See *id.*

[1911] China Steps Up Automobile Data Protection, *supra* (CHINA DAILY) (noting that this regulation is "a move to protect drivers' privacy and safeguard national security as vehicles are becoming increasingly digitalized in the world's largest auto market"; quoting a senior official at the CAC: "(The aim is) to cut disorderly collection and illegal use, but encourage its efficient use to facilitate the sector's healthy development.").

With a broad jurisdiction, this regulation applies to a wide range of automotive market players (defined as "automotive data processors") in China—including automobile manufacturers, components suppliers, software suppliers, distributors, dealers, repairers, and ride-hailing service firms—provided that the automotive data processing activities occur in China.[1912] "Automotive data" includes "personal information" and "important data" involved in the design, manufacture, sales, use, and maintenance of vehicles.[1913] Under the regulation, "personal information" refers to all the information related to identified or identifiable vehicle owners, drivers, passengers, and individuals outside the vehicles.[1914]

Likewise, the regulation clarifies the vague concept of "important data" in the automobile sector. To that end, it explicitly lists five categories of such data, including: (i) geographical information, or information about the passenger or traffic flows in important, sensitive areas (such as military zones, the locations of national defence technology firms or governmental bodies); (ii) data reflecting economic operations, such as vehicle flows and logistics; (iii) operation data of electronic vehicle charging networks; (iv) outside-the-vehicle video and image data, such as information related to human face and license plates; and (v) personal information involving more than 100,000 data subjects.[1915]

Substantively, the regulation establishes an overarching set of data protection principles to govern the processing of automotive data in general,[1916] as well as tailored regulatory standards for the treatment of personal information and important data, respectively.[1917] On top of China's general data protection framework, these sector-specific principles and standards further constrain and discipline the collection and processing of automotive data. As regards cross-border data transfers, the following aspects are most notable.

To begin with, the regulation provides that important data in the automobile sector (including personal information of 100,000 individuals) must be stored within China, and requires cross-border transfers of such data to pass the security assessments organized by the CAC along with other sector-specific regulators.[1918] To export important data as such, automotive data controllers shall strictly follow the permission granted out of the security assessments, if any, and must not exceed the purposes, scope, means of the transfers and the categories and scale of the data, as specified in the assessment decisions.[1919] When the CAC and other regulators launch compliance investigations and checks, automotive data controllers are obliged to cooperate with Chinese authorities, and shall provide them with the important data transferred abroad in a readable or otherwise convenient form.[1920]

[1912] Automobile Regulation, art. 3.
[1913] *Id.*
[1914] *Id.*
[1915] *Id.*
[1916] *Id.*, art. 6 (the regulation stipulates four principles to govern automotive data processing in general: in-car processing, no collection by default, proper precision, and anonymization).
[1917] See e.g., *id.*, arts. 7-14.
[1918] *Id.*, art. 11.
[1919] *Id.*, art. 12.
[1920] *Id.*

As for outbound transfers of personal information falling outside the ambit of "important data", they are governed by general rules on cross-border data transfers.[1921] This means that if the automotive data controllers do not constitute "CII operators" or trigger the CAC's volume thresholds, they may use certification or standard contractual agreements to export personal data in the automobile sector; otherwise, they are obliged to pass CAC-organized security assessments.[1922]

Further, the regulation imposes additional compliance duties on automotive data controllers handling important data. Specifically, it requires such controllers to perform risk assessments when processing important data, and to submit those reports to regulatory authorities.[1923] Also, controllers who process important data shall file an annual report to Chinese authorities to report on particulars on their data processing activities.[1924] Where controllers have transferred important data abroad, they must also include additional information specific to such transfers in the annual reports, such as the basic information of the overseas recipients, the categories, volumes, storage location(s), and retention periods of the data transferred, as well as the purposes and necessity of the transfers.[1925]

In addition to the Automobile Regulation, other regulatory authorities have also released sectoral rules to regulate the processing of data by smart cars. For instance, in July 2021, the *Ministry of Industry and Information Technology* (MIIT) issued a set of opinions, requiring manufacturers of smart and connected vehicles to domestically store personal information and important data collected and generated in China (unless passing security assessments).[1926] While this instrument seems to impose stricter requirements of data storage than the Automobile Regulation, it may suggest that the MIIT treats smart car manufacturers as "CII operators", to which the CSL's data localization obligation applies.[1927]

With these regulations in place, the automotive industry becomes a sector governed by dedicated data protection rules, including more stringent regulatory standards for cross-border data transfers. While they are only a recent example of sector-specific rulemaking, this trend might not stop at this sector. As the process of informatization proceeds and goes deeper, more sectoral regulations to implement the CSL, DSL, and PIPL are likely to follow.

C. Cybersecurity Review over Foreign Listings of Chinese Digital Platforms

---

[1921] *Id.*, art. 11.
[1922] PIPL, arts. 38, 40; Security Assessments Measure, art. 4.
[1923] *Id.*, art. 10. The report should detail (i) the type, quantity, scope, storage location(s) and retention periods, methods of use of those important data transferred; (ii) data processing activities; (iii) whether the data are to be shared with a third party, and (iv) data security risks and corresponding measures. *Id.*
[1924] *Id.*, art. 13.
[1925] *Id.*, art. 14.
[1926] MIIT, *Opinions on Strengthening the Governance of Smart and Connected Automotive Manufacturers and Product Access*, July 30, 2021, http://www.gov.cn/zhengce/zhengceku/2021-08/12/content_5630912.htm.
[1927] Xinhua Zhao and Mark Schaub, *China Issues New Rules on Data Security in Auto Industry*, KING & WOOD MALLESONS INSIGHTS (August 24, 2021), https://www.kwm.com/cn/en/insights/latest-thinking/china-issues-new-rules-on-data-security-in-auto-industry.html.

Aside from strengthening regulation in the automobile sector, the CAC also increasingly attaches importance to scrutinizing Chinese digital platform companies collecting and processing vast amounts of personal information, aimed to fence off those data from foreign governments' potential access and control. This trend is best manifested from the CAC's new rules of cybersecurity review for online platforms listing abroad.

By way of background, in April 2020, the CAC, along with 11 central ministerial departments, jointly issued the *Cybersecurity Review Measures* ("CRM 2020") to establish the cybersecurity review mechanism for CIIs.[1928] Under a mandate of the CSL,[1929] this mechanism was originally designed to review CII operators' procurement of network products and services,[1930] in order to identify and guard against relevant national security risks.[1931] In so doing, it aims to safeguard the security of CIIs' supply chains, which are deemed essential for protecting national security.[1932] Under the CRM 2020, the cybersecurity review office—an agency housed in the CAC—was mandated to implement and organize cybersecurity review process.[1933] Under the leadership of the *Central Cybersecurity and Informatization Commission* ("Central Commission"), the 12 ministerial departments that collectively issued this regulation constitute and function as a multi-ministry taskforce for the cybersecurity review mechanism, vested with significant regulatory and decision-making authority.[1934] Since July 2021, the cybersecurity review mechanism went through a drastic reconfiguration, which significantly expanded its jurisdiction and sharpened its regulatory scrutiny.

(A) The Domino Effect Generated by Didi's U.S. Listing

Following the initial public offerings of Didi (a giant Chinese ride-hailing service provider) at New York Stock Exchange (NYSE) on June 30, 2021, the cybersecurity review office launched a high-profile investigation over Didi on July 2, highlighting national security concerns over its data processing activities.[1935] On July 4 and July 9, it ordered Chinese app stores to remove a total of

---

[1928] *Measures for Cybersecurity Review*, issued on April 13, 2020, effective on June 1, 2020, https://cset.georgetown.edu/publication/measures-for-cybersecurity-reviews/ [CRM 2020]. These 11 ministerial departments include the National Development and Reform Commission, MIIT, Ministry of Public Security, Ministry of State Security, Ministry of Finance, Ministry of Commerce, People's Bank of China, State Administration for Market Regulation, State Administration of Radio, Film and Television, National Administration of State Secrets Protection, and State Cryptography Administration. See *id.*

[1929] Article 35 of the CSL required the CAC to implement and organize national security review for CII operators' procurement of network products and services that may affect national security. The CMR 2020 was designed to implement this requirement. See CSL, art. 35.

[1930] CRM 2020, art. 2 ("where a CII operator purchases network products or services that affect or are likely to affect national security, it must apply for cybersecurity review"). Under this regulation, "network products and services" refer to core network equipment, important communication equipment, high-performance computers and servers, mass storage equipment, large-scale databases, application software, cybersecurity equipment, cloud computing services, as well as other network products and services having a major impact on CII security. See *id.*, art. 20.

[1931] *Id.*, arts. 2, 5, 9.

[1932] 2020 Cybersecurity Review Measures, art. 1.

[1933] *Id.*, art. 4.

[1934] *Id.*, art. 4, arts. 11-12 (describing the decision-making authority), art. 15 (describing the authority to launch cybersecurity review process *ex officio*).

[1935] *Cybersecurity Review Office: Launching Cybersecurity Review against "Didi Chuxing" and Stopping Registration of New Users During the Investigation Process*, XINHUA NET (July 2, 2021), http://www.xinhuanet.com/legal/2021-07/02/c_1127618621.htm (according to the cybersecurity review, this

26 apps of Didi for its "grave problems on the collection and use of personal information in breach of PRC laws and regulations."[1936] On July 5, the cybersecurity review office also initiated cybersecurity review processes over three other Chinese Internet platform companies that had recently listed in the U.S.: two truck-hailing service providers (Yunmanman and Huochebang), as well as an online recruitment firm (Boss Zhipin).[1937] While none of these investigations involved the procurement of network products or services (nor was any of these companies officially identified by Chinese authorities as a "CII" operator), the CAC ordered cybersecurity review *ex officio*, citing national security concerns over the underlying data security risks.

On July 10, the CAC released a draft revision of the *Cybersecurity Review Measures*, aimed at institutionalizing cybersecurity review process for Chinese digital firms listing abroad.[1938] Most of the new rules were adopted by the final version of the *Cybersecurity Review Measures (2021)* ("CRM 2021"), which became effective on February 15, 2022.[1939] Different from the CRM 2020, the new rules expand the scope of cybersecurity review to cover network platform operators whose data processing activities affect or are likely to affect national security.[1940] This revision is made under a mandate of the DSL, which requires the establishment of the data security review mechanism to scrutinize data processing activities having national security impacts.[1941]

More specifically, the CRM 2021 requires network platform operators holding personal data of more than 1 million users (as a volume threshold) to apply for a cybersecurity review before listing on a foreign stock exchange.[1942] As defined by another 2021 draft regulation of the CAC, "network platform operators" generally refer to data processors that supply users with information dissemination, social networking, transaction, payment, audiovisual, and other digital platform services.[1943]

(B) The Policy Rationale

---

cybersecurity review process was launched to "prevent national data security risks, protect national security, and safeguard public interests.").

[1936] *Cyberspace Administration of China: Decision Concerning the Removal of "Didi Chuxing" App*, XINHUA NET (July 2, 2021), http://www.xinhuanet.com/legal/2021-07/04/c_1127621838.htm; *Cyberspace Administration of China: Removal of 25 Apps of Didi*, BEIJING DAILY (July 9, 2021), https://news.bjd.com.cn/2021/07/09/125333.shtml.

[1937] CAC, *Notice of the Cybersecurity Review Office to Launch Cybersecurity Review over "Yunmanman", "Huochebang", and "Boss Zhipin"*, July 5, 2021, http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm (the cybersecurity review office's grounds for launching these investigations were the same as those for Didi's case: to "prevent national data security risks, protect national security, and safeguard public interests.").

[1938] *Cyberspace Administration of China Issued Cybersecurity Review Measures (Revised Draft) to Solicit Public Comments*, SINA FINANCE (July 10, 2021), https://finance.sina.com.cn/china/gncj/2021-07-10/doc-ikqcfnca6037002.shtml.

[1939] *Cybersecurity Review Measures*, issued on December 28, 2021, effective on February 15, 2022, http://www.cac.gov.cn/2022-01/04/c_1642894602182845.htm. The CRM 2021 changed the draft measures' reference of "data controllers" to "network platform operators". See eg., *id.*, arts. 2, 7.

[1940] *Id.*, art. 2.

[1941] CAC, *Press Release on the Cybersecurity Review Measures*, January 4, 2022, http://www.cac.gov.cn/2022-01/04/c_1642894602460572.htm [CAC Press Release]. See DSL, art. 24.

[1942] CRM 2021, art. 7.

[1943] CAC, *Draft Network Data Security Management Provisions (Released for Comments)*, November 14, 2021, art. 73(9), http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm [*Draft Network Data Security Management Provisions*].

Though many Chinese Internet companies have listed in the U.S. stock market to raise capital for China's ICT-related sectors since the 2000s,[1944] Chinese authorities grew increasingly wary towards digital platforms holding vast troves of data since the case of Didi, tightening regulatory scrutiny over their offshore listings under national security grounds.[1945] As these data controllers increasingly amass huge amounts of personal information and important data collected and generated in China, PRC regulators were deeply concerned that foreign listings may enable another state to access and control such data, in ways that threaten China's data security and national security.

This stance is consistent with the China's growing emphasis on data security, which was treated by the 2021 DSL as an important component of national security.[1946] As noted earlier, with the prime role of data for achieving informatization recognized by PRC political leadership, ensuring national data security is guarding China's 'fundamental strategic resource' against various hostile forces.[1947] On the other hand, in the aftermath of Snowden revelations, the continuously deteriorating U.S.-China bilateral relationship, the U.S.-initiated trade war with China, as well as intensified U.S. economic sanctions on leading Chinese tech firms (e.g., Huawei, ZTE) had further strengthened China's security-oriented mindset.[1948] Such geopolitical and geo-economic dynamics have bolstered China's determination to safeguard large troves of Chinese data from being accessed by U.S. authorities. In this context, it is not difficult to understand China's salient national security concerns in the Didi's case: by choosing to list on a U.S. stock exchange, a digital platform giant like Didi essentially subjects itself to the jurisdiction of the U.S. government, facilitating the latter in accessing a myriad of personal information and important data harvested in China.[1949]

On the part of China, such a perceived national security threat culminated with the enactment of new submission and disclosure rules by U.S. Securities and Exchange Commission ("SEC"). On December 2, 2021, the SEC adopted amendments to finalize rules that implement the *Holding*

[1944] Serena Y. Shi, *Dragon's House of Cards: Perils of investing in Variable Interest Entities Domiciled in the People's Republic of China and Listed in the United States*, 37 FORDHAM INT'L L. J. 1265, 1278-79 (2014) (noting that since the 2000s, more than 100 PRC-domiciled companies have had listed in the U.S. through the use of VIE structures, "including most of the crown jewels of the PRC's Internet industry"; and that this was because U.S. listing enabled them to access the much-needed funding, and that being listed on a U.S. exchange also boosted the reputation and prestige of a company).

[1945] *Why Didi's Removal from App Win Public Support: Global Times Editorial*, GLOBAL TIMES (June 5, 2021), https://www.globaltimes.cn/page/202107/1227859.shtml?id=11 ("No internet giant is allowed to become a super database that has more personal data about the Chinese people than the country does, not to mention using the data at its own will…. For companies like Didi which have gotten listed in the US market and whose largest and second largest shareholders are foreign companies, China should more strictly supervise their information security to protect both personal data security and national security.").

[1946] In June 2021, the DSL was adopted, which elevates data security to a matter of national security. See DSL, art. 4 ("To safeguard data security, we should implement a holistic national security view").

[1947] See *infra* section I.C.

[1948] Creemers, *supra* (Book), 118.

[1949] See Li Qiaoyi & Zhang Hongpei, *3 More Internet Firms Scrutinized Amid Rising Data Security Concern*, GLOBAL TIMES (June 5, 2021), https://www.globaltimes.cn/page/202107/1227899.shtml ("The hypothetical scenario of the US coercing Chinese firms to submit data could happen, experts said, citing the US government's track record of stopping at nothing to forcing businesses to surrender.… Foreign Minister spokesperson Wang Wenbin said that time and again, it has been demonstrated that it is the US that forces companies to open "back doors" and illegally obtain user data.").

Foreign Company Accountable Act (HFCAA).[1950] The HFCAA requires foreign firms listed in the U.S. to comply with the audit standards of the Public Company Accounting Oversight Board (PCAOB), obliging them to provide the PCAOB with an audit primer within a specified timeframe.[1951] Under such new rules, a China-based U.S. listed company may be required to provide its data sets to U.S. regulators, and non-compliance with this obligation may result in regulatory sanctions, ranging from trading restrictions to delisting.[1952] As considered by the Chinese government, these rules would further consolidate and institutionalize U.S. authorities' access to Chinese firms' data, translating into a systemic vulnerability endangering China's national security.[1953] In this context, the CRM 2021 was widely regarded as Chinese authorities' strategic response to the HFCAA, explaining the adoption, timing, and substance of this new regulation.[1954]

Through the revamped cybersecurity review mechanism, PRC regulators strive to identify and address potential national security risks implicated in Chinese digital platforms' foreign listings, preventing potential transfers and provisions of sensitive and important domestic data to a foreign government like the U.S. Even if such data processing activities might occur outside China, the DSL applies to the extent that they may endanger China's national security interests, evincing significant extra-territorial effects.[1955]

(C) New Rules of Cybersecurity Review

Under the CRM 2021, the reconfigured cybersecurity review mechanism brings a wider range of data controllers under its jurisdiction, characterized by a broad scope of application. As noted earlier, all network operators handling personal data of more than 1 million users must apply for a cybersecurity review prior to listing in a foreign exchange.[1956] As the rules do not specify the types of "listings" subject to a cybersecurity review, a literal interpretation suggests that all forms of public listing abroad would trigger a mandatory review, if the volume threshold is met.[1957] These include initial public offerings (IPOs), listings through special purpose acquisition companies (SPACs), listings through a variable interest entity (VIE), direct or indirect listings, or reverse takeovers.[1958] Given that the 1 million threshold is relatively easy to reach for a large online platform in China, the CRM 2021 virtually imposes the cybersecurity review mechanism as an *ex ante* procedure by default for most Chinese tech giants planning to list abroad.[1959]

[1950] *SEC Adopts Amendments to Finalize Rules Relating to the Holding Foreign Companies Accountable Act*, U.S. SEC PRESS RELEASE (December 2, 2021), https://www.sec.gov/news/press-release/2021-250.
[1951] Hui Xu et al., *China Issues New Rules on Cybersecurity Review for Network Platform Operators Listing Abroad*, LATHAM & WATKINS CLIENT ALERT COMMENTARY (March 4, 2022), at 4, https://www.lw.com/admin/upload/SiteAttachments/Alert%202934.v5.pdf ["*Cybersecurity Review*"].
[1952] *Id.*
[1953] *Id*.
[1954] *Id.*
[1955] See DSL, art. 2 ("When *data processing activities conducted outside the territory of China undermine the national security*, the public interests, or the lawful rights and interests of citizens or organizations of China, legal responsibility is to be pursued in accordance with law.") (emphasis added).
[1956] CRM 2021, art. 7.
[1957] Xu et al., *supra* (*Cybersecurity Review*), at 3.
[1958] *Id.*
[1959] *Id*. The 1 million threshold is relatively low, given that China's online population is about 1.04 billion in 2022. See *supra* note 1.

Further, any member organization of the multi-ministry taskforce has the authority to *ex officio* initiate a cybersecurity review, where it considers that any entity's data processing activities affect or are likely to affect national security.[1960] This means that such a discretionary review may apply to a data controller that is not a typical network platform operator, or to a network platform operator processing personal data below the 1 million volume threshold. Meanwhile, Chinese companies listing in Hong Kong can also trigger a cybersecurity review, if the authorities identify national security concerns from the proposed deal (despite that a Hong Kong listing does not belong to a 'foreign listing' in a strict sense).[1961]

Substantively, the cybersecurity review process focuses on assessing risk factors that implicate national security interests.[1962] In addition to pre-existing elements relevant to CIIs' procurement and supply chain management under the CRM 2020, the new regulation increased two risk factors: (i) theft, disclosure, damage, illegal use, or export of core data, important data, or large amounts of personal information, and (ii) control of, access to, or malicious use of those data by a foreign government after listing on a foreign stock exchange.[1963] Focused on data processing activities posing national security threats, these two factors are intended to identify data security risks arising from a foreign government's unauthorized access to and control of massive sensitive or important Chinese data. Moreover, Chinese authorities may also consider "any other factors that may endanger the safety of CIIs, cybersecurity, or data security" during the review.[1964]

Procedurally, the cybersecurity review process consists of two steps. First, the cybersecurity review office decides whether to launch the review, and if so, will reach a preliminary decision.[1965] Second, the member organizations of the multi-ministry taskforce and relevant regulatory authorities would reach a unanimous decision on adopting the preliminary decision.[1966] Where their opinions split, a special review procedure will apply: the cybersecurity review office will draw input from relevant organizations and departments, and then reach a new decision to be approved by the Central Commission.[1967] Under the CRM 2021, the multi-ministry taskforce added the China Securities Regulatory Commission as a new member organization,[1968] which is the major regulator of the securities industry. In the review process, if Chinese authorities determine that there exists a national security concern, they will block the proposal of a foreign listing.[1969]

Under the regulation, companies need to obtain cybersecurity review clearance before submitting a listing application to foreign securities regulators.[1970] But the review process can take quite a

[1960] CRM 2021, art. 16(1). To launch such an investigation *ex officio*, the cybersecurity review office shall obtain the approval of the Central Commission. See *id.*
[1961] Xu et al., *supra* (*Cybersecurity Review*), 3.
[1962] CRM 2021, art. 10.
[1963] *Id.*
[1964] *Id.*
[1965] *Id.*, art. 11.
[1966] *Id.*, art. 12.
[1967] *Id.*, art. 13.
[1968] *Id.*, art. 4.
[1969] CAC Press Release, *supra*. Where an applicant fails the cybersecurity review, it is unclear whether the applicant can remedy the national security threats identified and re-file for another application.
[1970] *Id.*

long time: the normal review procedure may take a total of 55 working days (extendable by 15 working days); and the special review procedure may take another 90 working days (subject to discretionary extensions with no cap in a complex case).[1971] In other words, it may take 160 working days or even longer to complete the process in an exceptional scenario. During the cybersecurity review, an applicant is required to adopt measures to mitigate and remove relevant risks imposed to cybersecurity and data security.[1972]

Though the government has repeatedly stated that it does not intend to prohibit Chinese companies from listing abroad, the new cybersecurity review mechanism has substantially reinforced regulatory scrutiny and governmental control over such transactions from a national security and data security perspective.[1973]

First, the cybersecurity review process empowers Chinese authorities (led by the CAC) to veto digital firms' proposed overseas listings, provided that they identify national security threats arising from foreign governments' potential access to sensitive personal information or important data. Second, as the window for an overseas listing can be relatively short for a given company, a prolonged cybersecurity review can, in effect, destabilize the whole transaction, thereby deterring firms from making the listing application in the first place. Third, during the review process, the CAC typically orders a Chinese applicant to adopt risk mitigation and preventive measures, including suspension of new user registration and removal of apps from software application stores. Such measures may severely disrupt a company's daily business operations, adversely impacting its revenues and market shares.

Given the additional regulatory hurdles, costs, and uncertainties for foreign listings, it is not very surprising that the previous salient trend of Chinese firms listing on a U.S. exchange encountered a sudden stagnation since July 2021, witnessing the cancellation of many proposed IPOs.[1974] In the wake of China's cybersecurity review processes and the U.S. HFCAA, many Chinese companies now consider listing in Hong Kong, instead of the U.S. market, and Didi eventually delisted from the NYSE in June 2022.[1975]

D. Draft Network Data Security Management Provisions to Implement the CSL, DSL, and PIPL

In parallel to the enactment of the CRM 2021, the CAC also issued the *Draft Network Data Security Management Provisions* in November 2021.[1976] As a general regulation to implement the

---

[1971] *Id.*, arts. 9, 11, 12, 14. In addition, if the Chinese authorities demand the provision of supplementary materials from a party, the time spent to produce such documents does not count into the review timeline. *Id.*, art. 15.
[1972] *Id.*, art. 16(2).
[1973] Hui Xu et al., *supra* (*Cybersecurity Review*), 8.
[1974] Jianping Lei, *A Year After the Suspension of U.S. IPOs of China Concept Stocks*, REDIAN (July 10, 2022), https://redian.news/wxnews/43381.
[1975] *Id.*; Cissy Zhou, *Didi to Exit NYSE on June 10 Amid Uncertainty about China Restart*, NIKKEI ASIA (June 9, 2022), https://asia.nikkei.com/Business/Transportation/Didi-to-exit-NYSE-on-June-10-amid-uncertainty-about-China-restart (noting that Didi's shareholders overwhelmingly voted in favor of delisting on May 2022 after the Chinese authorities made it clear that "they would not lift a ban on adding new customers unless Didi first left the NYSE"; and that "[d]ozens of other Chinese companies have been notified by the U.S. (SEC) that (they) could be delisted by 2024 unless regulators are able to get full access to their audit records, which Beijing does not currently allow.").
[1976] *Draft Network Data Security Management Provisions*, *supra*.

CSL, PIPL, and DSL, it intends to concretize and clarify many regulatory requirements of these three legislations, particularly with respect to data security. Meanwhile, the draft regulation also contains several new rules to regulate data processing activities in China, enhancing the government's regulatory control over the processing of important data and personal information.

First, it clarifies the relationship between personal information and important data, and imposes additional regulatory requirements for certain controllers handling personal information. While the draft regulation does not explicitly list personal information as an enumerated category of "important data",[1977] it requires data controllers processing personal information of more than *1 million* individuals to comply with the regulatory requirements for processing important data.[1978] In other words, the draft regulation implicitly treats personal information above this volume threshold as a specific form of important data, and elevates the protection standards (including cross-border data transfer requirements) to the same level as those for the latter. A caveat to this default rule, however, is that sector-specific regulations may adopt different volume thresholds. For instance, under the Automobile Regulation, personal information of more than *100,000* data subjects constitutes "important data", triggering stricter regulatory requirements of the latter.[1979]

Second, the draft regulation imposes new obligations and regulatory requirements on data controllers of important data and large amounts of personal information. To begin with, it requires large network platform operators[1980] to report to the CAC and industry regulators, when establishing headquarters, operation centers, or research and development centers outside China.[1981] Likewise, the draft regulation obliges data controllers processing important data or personal information of over 1 million individuals to report to industry regulators or the local CAC, when they undergo restructuring (including mergers, reorganizations, and separations) or dissolution, or are declared bankruptcy.[1982] Given that restructurings often occur in the course of a company's overseas listing, this reporting obligation may be easily triggered in that context.[1983]

Moreover, the new rules require data controllers processing important data or listing abroad to conduct annual data security assessments—either in the form of self-assessments or through a qualified third party—and to file the reports of the previous year to the local CAC by the end of January each year.[1984] The annual assessment reports should include information relating to (i) the processing activities of important data, (ii) data security risks identified and corresponding

[1977] See *id*., art. 73(3) (categorizing "important data" as (i) governmental data, (ii) export control data, (iii) national economic data, business data of important industries, and statistical data, (iv) production and operation data of key industries and sectors, (v) national basic data relating to population, health, natural resources, and the environment, (vi) operational and security data pertaining to national infrastructure and CII, geographic and security data concerning important and sensitive areas).
[1978] *Id*., art. 26.
[1979] Automobile Regulation, art. 3.
[1980] A "large network platform" refers to an online platform that (i) has a minimum of 50 million active users in China during the previous year, (ii) has a market capitalization (valuation) of a minimum of 100 billion yuan by the end of the previous year, and (iii) has an outstanding performance in its main business and a strong ability to limit merchants' access to consumers (users). See State Administration for Market Regulation, *Draft Classification Guideline for Online Platforms*, October 29, 2021, https://www.samr.gov.cn/hd/zjdc/202110/t20211027_336137.html.
[1981] *Draft Network Data Security Management Provisions*, art. 13(2).
[1982] *Id.*, art. 14.
[1983] Xu et al., *supra* (*Cybersecurity Review*), 7.
[1984] *Draft Network Data Security Management Provisions*, art. 32(1).

measures, (iii) data security management system, (iv) compliance with PRC data security rules and standards, (v) security assessments of data sharing, trading, entrusted processing, and cross-border data transfers, among others.[1985] In addition, the draft regulation also obliges data controllers that have transferred personal information and important data abroad to file annual data export security reports to the local CAC.[1986] Such reports should detail the particulars relating to the overseas data recipients, the data transferred abroad, onward transfers (if any), and data security incidents.[1987]

Further, compared with the CRM 2021, the draft regulation further expands the jurisdiction of a mandatory cybersecurity review. To begin with, it explicitly requires data controllers proposing to list in Hong Kong to file for a cybersecurity review, where the listing affects or is likely to affect national security.[1988] While under the CRM 2021 Chinese authorities also may launch a discretionary review *ex officio* over this scenario, this provision turns this process into a mandatory review, requiring the company to apply for such a review.

In addition, under the draft regulation, network platform operators holding large amounts of data concerning national security, economic development, or public interests must apply for a cybersecurity review before mergers, reorganizations, and separations that affect or are likely to affect national security.[1989] While the exact scope of such data remains to be further clarified,[1990] this provision reflects the CAC's national security concerns over potential transfers of sensitive data during corporate restructurings, thereby subjecting such business transactions to its regulatory approval as a precondition.[1991]

In short, these new rules impose stricter compliance responsibilities and regulatory standards on data controllers holding important data and large troves of personal information, evincing the CAC's unwavering commitments to data security and cybersecurity as a regulatory focus—especially against unwarranted foreign access to such data.

Finally, under the rubric of "security management of cross-border data flows", this instrument mandates the establishment of "transborder data security gateway", blocking the dissemination of overseas-originated information prohibited by PRC laws in domestic cyberspace.[1992] As the first explicit reference to the "Great Firewall" in formal rules of Chinese regulations, this provision prohibits individuals or organizations to provide software, tools, networks, or Internet services for others to penetrate or circumvent the Great Firewall, while imposing the legal obligation not to

---

[1985] *Id*.
[1986] *Id.*, art. 40.
[1987] *Id.* (stating the reports should detail the types, volume, and purposes of the data transferred abroad, the overseas storage localization, retention period, scope of usage, and means of usage of such data).
[1988] *Id.*, art. 13(1).
[1989] *Id*.
[1990] The Draft Regulation does not specify what constitutes "large amounts of data" or what data concerns "national security, economic development, or public interests". Textually, such data may refer to national core data, important data, as well as personal data above a certain volume threshold in sensitive sectors.
[1991] See Xu et al., *supra* (*Cybersecurity Review*), 7 (noting that presumably, failing the cybersecurity review may mean that the company cannot proceed with the proposed restructuring, and that any form of merger, reorganization, or separation of a company's overseas structures may fall into the scope of this provision).
[1992] *Draft Network Data Security Management Provisions*, Chapter 5, art. 41.

route domestic Internet traffic abroad.[1993] In essence, this new rule expressly prohibits the provision of VPNs (or equivalent tools) in China, the breach of which will incur legal liabilities (such as administrative fines, confiscation of illegal profits, suspension or termination of business operations, revocation of licenses).[1994]

As such, this provision not only codifies the pre-existing technological measures of Internet filtering and censorship (as a form of "infrastructural data governance")[1995] into formal rules, but also institutionalizes their operation by sanctioning the provision of digital tools to bypass the Great Firewall. The underlying policy objective is to establish a formal regulatory mechanism to solidify and entrench the Great Firewall, while reinforcing the CAC's enforcement powers to police online content against unwanted foreign influence as a cybersecurity threat.

VI. IMPLICATIONS OF CHINA'S REGULATORY APPROACH ON ITS INTERNATIONAL RULEMAKING

Having canvassed the evolution of Chinese domestic data governance regime, this Part proceeds to explore its implications for China's international rulemaking on cyber and data regulation. To illustrate such a profound influence, it analyzes two notable case studies—international trade negotiations (Section A) and transnational data privacy rulemaking (Section B).

A. International Trade Negotiations

At the multilateral forum, China's first encounter with digital regulation was a WTO dispute—*China-Publications* case—whereby the U.S. brought an action against its regulation of certain publications and audio-visual entertainment products.[1996] While the U.S. did not challenge China's online censorship *per se*, it claimed that the operation of this system had discriminated against U.S. firms, in that their imported products were under more burdensome content review requirements than China's domestic firms.[1997] This claim was favored by the Panel and upheld by the Appellate Body.[1998] With such an unpleasant experience, China was concerned that WTO negotiations on e-commerce may curtail its sovereign autonomy to regulate the Internet industry and cross-border data flows.[1999]

On the other hand, with its burgeoning domestic rules imposing heavy regulatory control over online content and digital information, the government's leeway for international trade

[1993] *Id*.
[1994] *Id.*, art. 66.
[1995] See Erie and Streinz, *supra*, 42 ("Infrastructural data governance highlights the extent to which the regulation of data flows is a function of the physical, digital, and platform infrastructures that shape the digital domain.")
[1996] WTO Panel Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/R, adopted January 19, 2010, paras. 4.72-4.83.
[1997] *Id.*
[1998] *Id.*, para. 8.2; Appellate Body Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/AB/R, Adopted on January 19, 2010. paras. 414-417.
[1999] Henry Gao, *Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China*, in ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW 298, 301 (Shin-yi Peng et al. eds, 2021) ["Across the Great Wall"].

negotiations is significantly constrained, requiring Chinese negotiators to reconcile the tensions between trade liberalization and its domestic regulatory approach. Collectively, these factors explain why China takes a rather defensive approach to the inclusion of cyberspace or data regulation in international trade agreements.

(A) WTO Negotiations

Such a guarded stance is evinced from China's submissions to the WTO's two major venues on e-commerce negotiations. At the WTO's *Work Programme on Electronic Commerce*, China proposed to limit the scope of e-commerce negotiations to trade in physical goods facilitated by the Internet, while ignoring the U.S.'s repeated calls for new rules on domestic regulations constituting novel trade barriers. In its submission to the WTO in November 2016, China proposed that e-commerce negotiations should focus on "cross-border trade in goods enabled by [the] internet, together with services directly supporting such trade in goods, such as payment and logistics services."[2000] Aligned with China's competitive advantage on e-commerce (i.e., trade in traditional goods via the Internet, rather than pure digital services or contents), this proposal reflects the interests of China as a leading goods exporter, and serves its domestic e-commerce market and dominant online platforms (such as Alibaba).[2001] Also, it directs the focus of e-commerce negotiations towards conventional border barriers (e.g., tariffs and customs procedures), and away from behind-the-border regulatory barriers (such as domestic cyber and data regulations) at the core of the U.S.'s concerns.[2002]

Meanwhile, in this submission, China stated that the current discussions of the *Work Programme on Electronic Commerce* were meant to "clarify and to improve the application of existing multilateral trading rules."[2003] Since the existing WTO rules are widely regarded as not specifically dealing with novel regulatory issues of free information flows and data localization, this position indicates China's intention to bracket negotiations of such new rules for digital trade.[2004] In contrast, China's submission focused on traditional issues of trade facilitation, transparency, and other issues at the service of goods-related e-commerce.[2005]

Subsequently, at the plurilateral venue of *WTO Joint Statement Initiative (JSI) on Electronic Commerce*, China reiterated and further developed its proposals for Internet-enabled trade in goods, while seeking to subordinate cross-border data flows to a state's domestic regulations in exercise of data sovereignty. Though initially reluctant to join U.S.-led JSI negotiations on e-commerce, China eventually jumped on the JSI's bandwagon in January 2019, hoping to shape the rules-making to its preferred terms (rather than being excluded from the process as in the TiSA

[2000] WTO Work Programme on Electronic Commerce, Communication from the People's Republic of China and Pakistan, JOB/GC/110/Rev.1, JOB/CTG/2/Rev.1, JOB/SERV/243/Rev.1, JOB/DEV/39/Rev. 1, November 16, 2016, at 1 ["China's Communication"]. This submission was made before the 11th Ministerial Conference.
[2001] Henry Gao, *Digital or Trade?, The Contrasting Approaches of China and US to Digital Trade*, 21 J. INT'L ECON. L. 297, 317, 321 (2018).
[2002] *Id.*, 316.
[2003] China's Communication, *supra*, 1.
[2004] Gao, *supra* (Across the Great Wall), 301.
[2005] China's Communication, *supra*, 2-3. See *id.* (noting that these include "digital certificates, electronic signatures, electronic authentication", among others).

negotiations).[2006] As one of the most active participants at JSI negotiations, China thus far has submitted four communications (among a total of fifty-two substantive submissions), with two of them particularly relevant for our discussion.[2007]

In its first submission made in April 2019, China stated its general position with regard to JSI negotiations on e-commerce.[2008] Specifically, it reiterated the negotiation focus of issues pertaining to "cross-border trade in goods enabled by the internet", particularly trade facilitation measures.[2009] With respect to "data flow" and "data storage", China argued that such issues should be subject to "more exploratory discussion" before entering WTO negotiations.[2010] Though recognizing the importance of "trade-related data flow"[2011] to trade development, China maintained that such "data flow should be subject to the precondition of security, which concerns each and every Member's core interests."[2012] On this basis, China considered it necessary that "data flow orderly in compliance with Members' respective laws and regulations", while avoiding referring to "free flow of data" as advocated by the U.S.[2013] In other words, China argued that companies' business needs underlying transnational data transfers should be subordinated to domestic laws, establishing the primacy of a host state's data sovereignty to pursue security interests.

Relatedly, China emphasized that JSI Members should bear in mind national differences (on industry development, historical and cultural traditions, and legal systems), and "respect each other's design of the electronic commerce development paths, and the legitimate right to adopt regulatory measures in order to achieve reasonable public policy objectives."[2014] Reflecting the core tenets of its "cyber sovereignty" principle, this proposal underscores each country's sovereignty prerogatives to independently adopt its Internet and data governance approach to the

---

[2006] Gao, *supra* (Across the Great Wall), 302-5 (noting that China, when realizing that the 76 JSI members were taking e-commerce issues seriously, decided to join the negotiations in January 2019 when the JSI moved to the plurilateral negotiation phase; and that "China learned its lesson the hard way when its attempt to join the TiSA negotiations was blocked by the USA, making it impossible for China to shape the rules on services trade, where e-commerce was a major issue."). According to the Chinese WTO Ambassador Zhang Xiangchen, China's participation at the JSI strived to reinvigorate the negotiation function of the WTO at a time of crisis, in order to boost the confidence of the international community on the multilateral trading system and economic globalization. Also, China hoped to play an active role in designing a flexible framework to reflect the reasonable demands of different parties, especially of the developing countries. See *WTO Members Signed a Joint Statement on Electronic Commerce*, XINHUA NEWS (January 25, 2019), https://perma.cc/CT5U-4L9J.

[2007] Gao, *supra* (Across the Great Wall), 305.

[2008] *Joint Statement on Electronic Commerce, Communication from China*, INF/ECOM/19, April 24, 2019 ["INF/ECOM/19"].

[2009] *Id.*, 2.

[2010] *Id.*, 4.

[2011] As argued by Henry Gao, China's mention of "trade-related aspects of data flow" is noteworthy. Rather than using "free flow of data" (as typically referred to in U.S. submissions to the WTO), China qualifies "data flow" with "trade-related aspects", suggesting its intention to exclude data flows without a trade nexus from discussion. This qualification can be used to "justify restrictions on data flows in sectors where China has not made a commitment, or even for those covered by existing commitments but are provided free of charge (such as Google's search engine services) as they are not technically 'traded'." See Gao, *supra* (Across the Great Wall), 308.

[2012] INF/ECOM/19, 4.

[2013] *Id.*

[2014] *Id.*, 3.

exclusion of foreign interference or pressure, and echoes China's call for all Members to safeguard cybersecurity.[2015]

As such, China seeks to extend and transplant its domestic narratives of cybersecurity and data sovereignty to the international level,[2016] aimed to establish the supremacy of national security over economic interests underlying cross-border data flows. Under this logic, there should be no unrestricted or "free" cross-border data flows by default. Rather, the terms and conditions for cross-border data flows must be determined by a state, which may deploy domestic regulations to ensure that its cybersecurity, data security, and national security interests are adequately protected before data export is allowed. In this way, cross-border data transfers for international trade purposes are subordinated to a state's data sovereignty.

In another submission made in May 2019, China articulated detailed proposals for its prioritized issues.[2017] Among the relevant provisions, China proposed a cybersecurity exception and a national security exception. As regards the former, China maintained that the new agreement on e-commerce shall allow "any measures for the purposes of guaranteeing cybersecurity, (and) safeguarding cyberspace sovereignty", subject to a three-prong test of non-arbitrariness/discrimination, non-trade-restrictiveness, and necessity.[2018]

In terms of the latter, China proposed that any Member must be allowed to adopt "any action which *it considers necessary for the protection of its essential security interest*."[2019] Crouched in self-judging language as such, this provision would blanketly shield a state's domestic Internet governance and data regulatory measures from international dispute settlement mechanism, provided that the government deems them necessary to guard against its perceived national security threats. By this virtue, China's commitments to cybersecurity and data sovereignty would become non-negotiable in international trade rulemaking and exempted from mandatory dispute resolution, since they are *ex ante* carved out from the realm of trade (or digital) "protectionism".

(B) Preferential Trade Agreements

As with its attitude on WTO negotiations, China also adopts a rather cautious approach to Internet and data regulation when concluding preferential trade agreements (PTAs), in order to safeguard its sovereign autonomy to implement such regulatory measures domestically. Though it has entered into more than a dozen PTAs, most of them contained no e-commerce chapters, and did not deal with such regulations at all.[2020] Prior to the conclusion of the *Regional Comprehensive Economic Partnership* (RCEP) in November 2020, there are only six Chinese PTAs with stand-alone e-commerce chapters.[2021] But in all these treaties, the e-commerce chapters mainly dealt with

[2015] *Id.* See *supra* section I.B.
[2016] Gao, *supra* (Across the Great Wall), 309.
[2017] *Joint Statement on Electronic Commerce, Communication from China*, INF/ECOM/32, May 9, 2019.
[2018] *Id.* ("provided that subject measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and are no more than necessary to achieve the objectives.").
[2019] *Id.* (emphasis added).
[2020] Gao, *supra* (Across the Great Wall), 298.
[2021] *Id.* (noting that these treaties are 2015 China-Korea PTA, 2015 China-Australia PTA, 2019 China-Mauritius PTA, 2020 China-Cambodia PTA, as well as the recently upgraded 2017 China-Chile PTA and 2018 China-Singapore PTA).

trade facilitation related issues, without any prescriptive language on cyber or data regulation.[2022] This prominent feature stands in stark contrast with new-generation U.S. PTAs, which typically use binding and enforceable language to establish regulatory requirements for free data flows and against data localization.[2023]

A notable exception to this trend of trade rulemaking, the RCEP (signed by China and other fourteen Asia-Pacific countries) represents a major breakthrough, as it adopted U.S.-designed template provisions on free data flows and data localization.[2024] By this virtue, China, for the first time in an international trade agreement, commits not to "prevent cross-border transfer of information by electronic means…. for the conduct of the business",[2025] and not to require the use or location of "computing facilities in (its) territory as a condition for conducting business."[2026] However, different from U.S.-promoted digital trade rules, such provisions of the RCEP are substantially qualified by a self-judging national security exception, allowing a state to adopt "any measure that it considers necessary for the protection of its essential security interests."[2027] And the implementation of such security measures "shall not be disputed by other Parties."[2028]

Meanwhile, under another exception, measures that a state "considers necessary to achieve a legitimate public policy" are also carved out from these two provisions,[2029] permitting the state itself to determine the necessity as such.[2030] Finally, the whole e-commerce chapter is carved out from mandatory dispute settlement mechanism under the RCEP,[2031] rendering these commitments judicially unenforceable.

While the "binding-yet-unenforceable" nature of these provisions seems paradoxical, they were the result of a compromise, struck between two competing positions on digital rules. While Japan built a coalition of like-minded negotiating countries early on to push for the adoption of U.S.-designed template to ensure free cross-border data flows and no data localization by default,[2032] China's insistence against such rules led to a key contention during the RCEP negotiations.[2033] Ultimately, China backed off and conceded to the incorporation of these provisions, partly due to

---

[2022] *Id.*; Henry Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, HENRICH FOUNDATION (January 18, 2022), at 14, https://www.hinrichfoundation.com/research/article/digital/data-sovereignty-trade-agreements-digital-kingdoms/.
[2023] Yakovleva, *supra*, 487-90.
[2024] RCEP, arts. 12.14(2), 12.15(2). Compare with CPTPP, arts. 14.11(2), 14.13(2).
[2025] RCEP, art. 12.15(2).
[2026] RCEP, art. 12.14(2).
[2027] RCEP, arts. 12.14(3)(b), 12.15(3)(b).
[2028] RCEP, arts. 12.14(3)(b), 12.15(3)(b).
[2029] RCEP, arts. 12.14(3)(a), 12.15(3)(a). Under this exception, such measures must satisfy the non-arbitrary, non-discrimination, and non-trade-restriction requirements. See *id.*
[2030] RCEP, arts. 12.14(3)(a) (fn.12), 12.15(3)(a) (fn.14).
[2031] RCEP, art. 12.17.
[2032] Oki Nagai, *Japan Teams with RCEP Allies to Push China on Data Free Flow*, NIKKEI ASIA (December 30, 2020), https://asia.nikkei.com/Economy/Trade/Japan-teams-with-RCEP-allies-to-push-China-on-data-free-flow ("Tokyo's basic strategy was to prevent a Beijing-led pace of negotiations. Given the difficulty of negotiating one-on-one with a global power like China, Japan sought to enlist other countries that shared the same goal, in what former Japanese deputy economic minister Takashi Shimada called a 'league of trustworthy partners.'").
[2033] *Id.* (noting that at an RCEP ministers meeting in May 2017, Japan "distributed a single-sheet handout with a proposal to cover digital rules in the negotiations", which China vigorously objected).

the pressure from the Japan-led coalition,[2034] and partly because it started to realize that such commitments actually align with its growing needs of facilitating inbound data flows from overseas Chinese tech firms for domestic commercialization of such data.[2035] However, leveraging its bargaining power, China successfully pushed for self-judging exceptions for "national security" and "legitimate public policy" purposes.[2036] Also, China's objections delayed a decision by negotiating countries to subject the RCEP's e-commerce provisions to mandatory dispute resolution, which failed to make it into the final agreement.[2037]

As a result, the RCEP's commitments on cross-border data flows and data localization not only may be prevailed over by a state's perceived national security, data security, and cybersecurity concerns, but also are unenforceable through international adjudication. While welcoming *inbound* data flows, China is allowed to self-determine which *outbound* data transfer restrictions and what domestic data localization requirements are necessary and justified.[2038] Through broad and sweeping carve-outs as such, China effectively exempts its internal cyber and data regulations from international adjudication altogether, maintaining almost unrestricted sovereign autonomy to safeguard its self-defined security and strategic interests. Overall, the RCEP's case evinces China's selective reshaping of U.S.-promoted digital trade template (originally designed to discipline its domestic data governance approach as "digital protectionism"),[2039] realigning such provisions with its policy preferences and national interests.[2040]

B. Transnational Data Privacy Rulemaking: The Case of the APEC CBPR System

In addition to international trade negotiations, China's domestic data governance regime has also considerably influenced its approach to transnational data privacy rulemaking. Most notably, such implications are manifested from China's attitude towards the *APEC Cross-Border Privacy Rules* (CBPR) system. Designed to implement the data protection principles of the *APEC Privacy*

[2034] *Id.*
[2035] See *supra* Chapter 1 ("A Battle of the Big Three?"), section IV.C.
[2036] *China's Evolving Data Governance Regime*, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (July 26, 2022), https://www.uscc.gov/research/chinas-evolving-data-governance-regime [USCC]; Nigel Cory, *Writing the Rules: Redefining Norms of Global Digital Governance*, in CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 85, NATIONAL BUREAU FOR ASIAN RESEARCH (March 2022), https://www2.itif.org/2022-NBRsr97-china-digital-ambitions.pdf?_ga=2.204751381.480101597.1652729267-2102500758.1652729267#page=79 (noting that in addition to China, "India also pushed for the self-judging national security exception" before it ultimately withdrew from the negotiations).
[2037] Nagai, *supra*.
[2038] Erie and Streinz, *supra*, 39.
[2039] Susan Ariel Aaronson, *What Are We Talking about When We Talk about Digital Protectionism*, 18 WORLD TRADE REVIEW 541, 555-56 (2019) ("The Obama administration wanted to create the rules and processes governing digital trade to 'promote the digital economy through a free and open Internet'. As the talks progressed, US trade diplomats became increasingly concerned about digital protectionism, recognizing that it could threaten the dominance of US internet giants, which require relatively unrestricted access to operate and build new businesses like artificial intelligence (AI) and apps. Hence, TPP parties banned certain types of practices that could fragment the internet, reduce access to information, and/or increase the cost and difficulty of doing business online. Given China's global influence as the second-largest economy and the country with the most internet users, Obama administration officials were also particularly concerned about China's efforts to enforce its concept of cyber-sovereignty…. From the US perspective, the TPP allowed the United States and its allies, rather than China, to set the rules regarding data flows.").
[2040] See Heng Wang, *Selective Reshaping: China's Paradigm Shifting in International Economic Governance*, 23 J. INT'L ECON. L. 583, 584 (2020).

Framework, the CBPR mechanism aims to provide an international solution to facilitate cross-border personal data flows.[2041] In a 2017 WTO submission against China's *Cybersecurity Law*, the U.S. argued that China, instead of imposing stringent conditions for cross-border data transfers, could and should allow the CBPR system to export personal data, which is a "less burdensome option" to "achieve privacy objectives."[2042] At the APEC's forum, the U.S. has long been acclaiming the CBPR as a "model for global interoperability among (different national) privacy regimes".[2043] In U.S.-led new-generation PTAs (such as the USMCA), the CBPR is recognized as "a valid mechanism to facilitate cross-border information transfers while protecting personal information."[2044] In April 2022, the U.S. initiated a campaign to establish a Global CBPR system,[2045] striving to upgrade the CBPR from an Asian-Pacific data transfer mechanism to a widely adopted international standard.[2046] However, China is unlikely to come on board. Though China is an APEC economy that endorsed the CBPR system in 2011, it has never expressed any interest in participating.[2047] Nor will it accept the CBPR as a legitimate mechanism for cross-border transfers of personal data. At the core, this position can be explained by the following factors.

First, for China, the level of data protection provided by the CBPR is quite insufficient,[2048] making it unable to safeguard the government's data security and national security interests underlying cross-border personal data flows. With only "a mild prescriptive bite",[2049] the *APEC Privacy Framework* stipulates a set of principles-based standards of data protection, which are often regarded by data privacy experts as too loose to adequately protect personal data.[2050] In addition, its substantive standards are subject to broad derogations by mandatory rules of national law,

---

[2041] APEC, *What is the Cross-Border Privacy Rules System*, October 2021, https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015 (explaining that the CBPR system "is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally-recognized data privacy protections.")

[2042] 2017 U.S. WTO Submission, *supra*, at 2, para. 3(c).

[2043] APEC, *APEC Cross-Border Privacy Rules System Goes Public*, NEWS RELEASE (July 31, 2012), https://www.apec.org/Press/News-Releases/2012/0731_cbpr.

[2044] See e.g., UCMCA, art. 19.8(6).

[2045] U.S. Department of Commerce, *Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum*, https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border; see U.S. Department of Commerce, *Global Cross-Border Privacy Rules Declaration*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

[2046] U.S. Department of Commerce, *Global Cross-Border Privacy Rules Declaration FAQ*, https://www.commerce.gov/sites/default/files/2022-04/Global-Cross-Border-Privacy-Rules-Declaration-FAQ.pdf.

[2047] Andrei Gribakov, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (January 3, 2019), https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

[2048] Yanqing Hong, *Understanding the Political and Economic Considerations Behind the APEC Cross-Border Privacy Rules System*, WANGAN XUNLUREN (October 4, 2017), https://mp.weixin.qq.com/s/Gi59sRKAftyYcPhTVFmkTQ.

[2049] LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 76 (2014).

[2050] *Id.* (noting that the standards of the APEC Privacy Framework are generally lower than European data protection law: "[f]or instance, the Framework does not embrace the sensitivity principle, and it applies the criteria of 'fair' and 'lawful' only to the *collection* of personal information (paragraph 18) as opposed to further stages of information processing as well"); Graham Greenleaf, *Five Years of the APEC Privacy Framework: Failure or Promise?*, 25 COMPUTER LAW AND SECURITY REVIEW 28 (2009); CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAWS 51 (2011).

which are allowed under relatively lax criteria.[2051] Obviously, these aspects are unacceptable to China. As noted earlier, through domestic regulations, China requires a data recipient country to implement high-standard protections to safeguard the security of domestically originated personal information, with its level of data protection being at the core of the CAC's security assessments.[2052] In particular, China may regard possible derogations in a recipient jurisdiction as a security loophole, enabling a foreign government (such as the U.S.) to access and control sensitive personal data in ways that undermine its perceived national security interests.

Second, China is concerned that the CBPR establishes too low a threshold for cross-border data flows, constraining its sovereignty prerogatives to require a recipient jurisdiction to provide a level of protection above the standards of the *APEC Privacy Framework*.[2053] Under the CBPR mechanism, certified firms are assumed to have complied with a unified set of cross-border data protection rules (stipulated in the *APEC Privacy Framework*), and thus are allowed to freely transfer personal data to another CBPR-compliant company across national borders.[2054] This means that among participatory economies of the CBPR, a data exporting country cannot restrict data transfers to a recipient jurisdiction with less strict data protection standards, even though it may consider such transfers as triggering data security or even national security risks.[2055] Given China's stringent and sophisticated regulatory requirements for cross-border data flows, the CBPR's threshold for data export seems too permissive. More importantly, by creating an important carve-out for CBPR-compliant companies to circumvent China's domestic data regulations, application of the CBPR would use a permissive international privacy floor to replace China's strict regulatory standards for data export, undercutting its sovereign autonomy to regulate cross-border data flows.

Third, from a geo-economic perspective, while widespread adoption of the CBPR by the international community can well serve the U.S.'s strategic interests, this is misaligned with China's prioritized interests underlying its pursuit of data sovereignty. As pointed out by Dr. Hong, through the CBPR system, the U.S. seeks to ensure that third countries would not restrict cross-border transfers of personal information due to divergent national data protection standards.[2056] Eventually, the strategic objective behind is to facilitate flows of personal data collected from different countries back to the U.S.,[2057] where most global tech giants and digital platforms are headquartered. This not only would benefit U.S. firms and digital industry (which will leverage those data to extract economic interests and spur technological innovation), but also can advance the U.S.'s surveillance interests (as U.S. signals intelligence agencies may access and tap on such information to achieve security and strategic goals).

However, the cost-benefit calculation for China is drastically different. Unlike their U.S. counterparts, a vast majority of top Chinese Internet companies almost exclusively serve the Chinese market, with most of their facilities and operations based in China.[2058] This explains why

[2051] BYGRAVE, *supra*, 76; see APEC Privacy Framework, para. 18.
[2052] See *supra* Sections III.B. and V.A.
[2053] Hong, *supra* (Understanding).
[2054] Gribakov, *supra.*
[2055] *Id.*
[2056] *Id.*
[2057] *Id.*
[2058] Gao, *supra* (Digital or Trade), 317.

they do not share the same demands for international rules on free data flows and against data localization as U.S. digital firms.[2059] On the other hand, if China joins the CBPR system, U.S.-based CBPR-compliant companies can freely transfer large troves of China-originated personal information (including important data) to the U.S. This will enable U.S. intelligence surveillance authorities to access and control such data, thus weaponizing this asset against China's national security and strategic interests. Unrestricted data flows under the CBPR can also consolidate and entrench the global dominance of American digital industry, undermining the competitive edge of Chinese firms in the U.S.-China tech race. In short, given their vastly divergent interests and concerns underlying cross-border data flows, China and the U.S. "stand on different sides of the CBPR."[2060]

CONCLUSION

This chapter delves into an important, yet understudied, issue—the evolution and development of China's domestic data governance regime. In this endeavor, it makes three contributions for enriching and deepening our understanding about the Chinese approach to data regulation.

First, it unpacks core normative substance of China's concepts of "cyber sovereignty" and "data sovereignty", anchored at the heart of its cyberspace governance system. Under the rubric of "cyber sovereignty", the PRC claims the exclusive right of the government to manage domestic Internet governance within its borders, free from any external interference. By invoking cyber sovereignty to legitimize its online content filtering and censorship, the Chinese government seeks to effectively control the flows of information available to its domestic online population, in order to safeguard its overarching political interests of regime security.[2061] As the paramount importance of data for economic growth, technological development, and social governance is increasingly recognized, the focus of China's cyberspace rulemaking has been shifting from online content management to data regulation.

Built on the notion of "cyber sovereignty", China's vision of "data sovereignty" strives to exert stringent regulatory control over various data processing activities implicating national data security, while asserting exclusive governmental authority over intra-country and cross-border data flows. In particular, China advocates for "data sovereignty" to challenge the global dominance of U.S. actors (whether private or public) over their unrivaled data collection capacity, safeguarding domestically originated data against unauthorized foreign access and control. By deploying the doctrine of data sovereignty, China seeks to preserve the security of data as a source of vulnerability for cybersecurity and national security, while leveraging big data as a "fundamental strategic resource" to achieve informatization and development goals. In lieu of Western liberal values or constitutional rights, China's domestic data governance regime is largely driven by the intertwined objectives of protecting national security (against risks arising from domestically stored and generated data), and fostering national economic and technological development (by utilizing the strategic asset of data).[2062]

[2059] *Id.*
[2060] Ron Cheng, *China's Cyber Sovereignty and Cross-Border Digital Trade*, LAWFARE (March 31, 2017), https://www.lawfareblog.com/china-cyber-sovereignty-and-cross-border-digital-trade.
[2061] Hellström, *supra*, 58.
[2062] Erie and Streinz, *supra*, 24, 85; Creemers, *supra* (Emerging), 2.

Second, this chapter traces the evolution of the Chinese legal and regulatory framework governing data security and cybersecurity, charting the institutional trajectory through which China's data governance regime came into shape. Rather than appearing overnight out of political whims, Chinese legislatures and regulations dealing with the treatment of data are the result of years of incremental rulemaking, constant evolution, and gradual institutional change (substantially accelerated after 2016), reflecting the party-state's strategic and coordinated regulatory responses to its perceived problems and policy priorities concerning "cybersecurity" and "informatization".[2063] Through the enactment of 2016 CSL, 2021 PIPL, and 2021 DSL, China has transformed erstwhile sectoral data regulations into a comprehensive legal architecture to establish data sovereignty. Focused on ensuring data security and cybersecurity, this new framework imposes horizontal data localization requirements on CII operators handling important data and personal information, as well as data controllers whose processing of personal information meets the statutory volumes.

By design, cross-border data transfers are allowed only if data exporters resort to relatively burdensome, costly, and inflexible mechanisms of security assessments, certification, or standard contractual agreements. In particular, transnational transfers of important data or large amounts of personal information must pass CAC-organized security assessments, subjecting these data flows to Chinese authorities' *ex ante* regulatory approval and *ex post* supervision and monitoring. Though these three transfer mechanisms are meant to facilitate cross-border data flows, their onerous requirements may generate considerable time delays, compliance costs, administrative burdens, and legal uncertainties, indirectly compelling companies with data-intensive businesses to rely on localized data storage and processing instead.

Institutionally, the CAC emerged as a powerful super regulator to spearhead and oversee online content management and data regulation, vested with consolidated regulatory authority and reinforced law enforcement powers. With a primarily security-focused mindset to pursue data sovereignty, the CAC not only pushed for ancillary regulations to implement the regulatory standards set forth by the CSL, PIPL, and DSL, but also established sector-specific rules to strengthen regulatory control and management of data in sensitive industries. Moreover, together with other sectoral regulators, the CAC has vigorously implemented national security review mechanisms to scrutinize transnational business transactions (including listings and restructurings) that may render sensitive and important Chinese data to a foreign government's potential access and control. By screening overseas data processing activities implicating national security risks as such, Chinese authorities expand the jurisdictional reach of China's data governance regime, while tightening regulatory oversight over cross-border transactions involving transfers of massive domestic data. In this way, China's territorial-based data regulations are generating significant extraterritorial effects.

Third, this work systemizes the implications of China's domestic data regulatory framework for other parallel international regimes governing cross-border data flows. With stringent regulatory control over online content and cross-border data flows, China's domestic data governance regime heavily influences its international rulemaking on e-commerce, digital trade, and data privacy protection. Though China has actively engaged with e-commerce rulemaking during international

[2063] Creemers, *supra* (Emerging), 2.

trade negotiations, it has long adopted a cautious and guarded approach when dealing with Internet or data regulation. Focused on negotiating broad, self-judging exceptions for national security purposes, China seeks to carve out its domestic cyberspace regulations (including online content management, data localization, and cross-border data transfer requirements) from international adjudication altogether, making trade treaties conform to its domestic data governance approach.

In addition, as shown by the RCEP that features "binding-yet-unenforceable" provisions for free data flows and against data localization, the PRC has selectively reshaped international trade rulemaking based on its policy preferences, repurposing U.S.-designed digital trade rules to serve its shifting national interests. In terms of transnational data privacy protection, China, given its strong commitments to "data sovereignty" and national security, is unlikely to accept the U.S.-promoted CBPR system as a valid mechanism for international personal data transfers. Thus, China and the U.S., as two economic behemoths worldwide, may not be able to bridge their drastic differences on data regulation in international trade and data privacy rulemaking in the near future.

With the implementation of a comprehensive data governance regime in pursuit of data sovereignty, China strives to wield strict regulatory control over data (particularly personal information and important data) in defense of national security interests, while using the resource of big data to drive economic growth and enhance the party-state's social control. Through a security-oriented set of domestic laws, institutions, and processes, Chinese authorities are empowered to determine regulatory standards for the treatment of data, making a powerful claim to govern the contentious matter of cross-border data flows.

Chapter 6

Policy Diffusion of the Chinese Approach to Cyber and Data Governance

Table of Content

I. INTRODUCTION 298

II. THIRD COUNTRIES' EMULATION OF CHINA'S CYBER AND DATA GOVERNANCE APPROACH 299

A. Vietnam's Cybersecurity Law 301

B. Myanmar's Draft Cybersecurity Law 302

III. "PUSH-AND-PULL" FACTORS UNDERLYING THIRD COUNTRIES' EMULATION 304

A. Chinese Government Advocating for Its Domestic Data Governance Approach Internationally 304

(A) Bracketing Security-Motivated Domestic Data Regulations in International Trade Negotiations 306

(B) Promoting Its Preferred Norms in Regional and International Institutions of Global Governance 307

(a) Engaging with Like-Minded Countries in Regional Inter-State Organizations 308

(b) Promoting Cyber Sovereignty at the World Internet Conference (the Wuzhen Process) 311

(c) Advocating for Global Initiative on Data Security on the International Stage 313

(d) Norm Promotion in International Institutions of Global Governance 316

B. Digital Silk Road: Chinese Technological Firms Acting as Infrastructural Agents 319

C. The Normative Appeal of Cyber and Data Sovereignty 323

(A) Cybersecurity and National Security Concerns 324

(B) Economic Interests and the Narrative of "Data Colonialism" 325

(C) Strategic Interests of Greater Participation in Global Internet Governance 327

(D) Caveats 328

D. Carving Out an International Trade Exception for Inbound Data Flows 330

IV. CONCLUSION 331

I. INTRODUCTION

In the past two decades, as the People's Republic of China (PRC) emerged as a major power with the second largest economy worldwide, it increasingly asserts itself in the international system,

striving to assume a more central and powerful role in global governance.[2064] To put it in the words of President Xi Jingping, China is determined to "lead the reform of the global governance system", shaping international order, institutions, and norms in ways that reflect its vision, interests, and priorities.[2065] In the unfolding digital era, Internet governance and data regulation are important components of these ambitious initiatives.

Domestically, the Chinese approach to cyberspace governance is characterized by stringent online content control (i.e., Internet filtering and censorship), comprehensive localized storage of different categories of data, and relatively onerous restrictions on cross-border data flows.[2066] Under the principles of "cyber sovereignty" and "data sovereignty", these regulatory and technical measures are implemented by Chinese authorities to safeguard cybersecurity and national security, while pursuing strategic interests underlying digital information flows.[2067] At the international arena, the Chinese government, aimed at transforming itself from a rule-taker to a rule-maker (i.e., a "cyber superpower")[2068], has been deploying a multifaceted strategy to advance its vision of cyber and data regulation, proactively shaping the transnational digital governance landscape based on its domestic norms, policies, and practices. To unpack the understudied policy diffusion of the "Chinese way" abroad, this paper surveys the mechanisms and factors animating third countries' emulation of the Chinese data governance approach in pursuit of "cyber" and "data sovereignty", explaining the rise of an institutional alternative alongside the U.S. and European models.

This chapter proceeds as follows. Section II outlines an increasingly salient trend of third countries imitating China's approach to data governance, exemplified by two case studies of Vietnam and Myanmar. Section III delves into the mechanisms and factors driving the diffusion of the Chinese regulatory approach in recipient countries. These include the Chinese government's international advocacy and norm promotion efforts, Chinese tech firms' export of digital infrastructures to emerging markets, and the normative appeal of China's vision of cyber and data governance. Section IV summarizes and draws conclusive remarks.

II. THIRD COUNTRIES' EMULATION OF CHINA'S CYBER AND DATA GOVERNANCE APPROACH

Though triggering many controversies and concerns, online content control emerges as a rising cyberspace policy and practice among more and more countries worldwide.[2069] Contrary to the first-generation vision of cyberspace as an open commons completely beyond sovereign reach, a

[2064] *China's Approach to Global Governance*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/china-global-governance/.
[2065] Xiangyang Chen, *General Secretary Xi Jinping's Thought on Global Governance*, PEOPLE DAILY ONLINE (August 17, 2017), http://theory.people.com.cn/n1/2017/0817/c83859-29476848.html (noting that Xi made this statement at a collective study session of the Politburo in October 12, 2015).
[2066] See *supra* chapter 5 ("China's Data Sovereignty"), section I.C.
[2067] *Id.*, sections I-II.
[2068] See *The First Meeting of the Central Leading Group for Cybersecurity and Informatization*, February 27, 2014, http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm.
[2069] Daniëlle Flonk, *Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control*, 97 INT'L AFFAIRS 1925, 1925 (2021).

growing number of countries today engage in Internet filtering and censoring for political and strategic goals, increasingly exerting governmental control on free flows of online information.[2070]

Likewise, while China is often criticized for its stringent measures to localize the storage and processing of data within its territory, recent empirical studies suggest that the policy of data localization is by no means limited to China.[2071] As revealed by an OECD trade policy paper published in June 2022, national data localization measures have been on the rise, with a clear upward trend in their total number.[2072] By 2021, there are 92 data localization measures across 39 countries that explicitly mandated domestic storage or processing of data, and more than half of them were adopted within the last five years.[2073] As a general trend, these data localization measures are becoming more restrictive over time: by 2021, two-thirds of these identified measures contained a domestic storage requirement with a prohibition on cross-border data transfers.[2074] Among all these measures, approximately 16% of them include prohibitions on transfers of personal data or "important data" (also termed as "critical data").[2075]

To be clear, existing national data localization measures vary widely. Motivated by different normative and policy objectives, they often apply different types of rules to different types of data (whether personal or non-personal, sector-specific or not).[2076] Among the measures identified by the OECD paper, the major motivations behind data localization include domestic data privacy protection, ensuring data access for regulatory purposes, national security purposes (for national security services, or to safeguard sensitive data against foreign surveillance), as well as protectionist purposes and industrial policies.[2077] Though all such measures contain explicit requirements of domestic data storage, the specific formulations often diverge, and their restrictions on cross-border data transfers differ considerably, ranging from no limitation to complete prohibition (*de facto* or *de jure*).[2078] While a comprehensive survey on such nuances is beyond the scope of this chapter, there is a notable trend that an increasing number of developing countries have been enacting, or are considering, domestic regulations that mirror the Chinese approach.

[2070] Ronald J. Deibert & Masashi Crete-Nishihata, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339, 339 (2012); See JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD viii, xiii (2006).

[2071] See e.g., Nigel Cory & Luke Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, 3, ITIF (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (noting that "China is the most data-restrictive country in the world"; and that "[d]ata-localization policies are spreading rapidly around the world…. The number of data-localization measures in force around the world has more than doubled in four years…. ").

[2072] Javier López González et al., *A Preliminary Mapping of Data Localisation Measures*, OECD TRADE POLICY PAPER (June 2022), at 8, https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en. There is no universally accepted definition of what is a "data localization" measure. The OECD paper defines "data localization" as any measures with "more *explicit requirement that data be stored and/or processed within the domestic territory*", avoiding the controversial issue whether emerging data privacy protection regulations that restrict cross-border personal data flows (such as the EU's GDPR) qualify as such. See *id.*, 4-5.

[2073] *Id.*, 8.

[2074] *Id.*

[2075] *Id.*, 9.

[2076] *Id.*, 6-7.

[2077] *Id.*, 6.

[2078] *Id.*, 6-7.

To illustrate this phenomenon of policy diffusion of Chinese norms, policies and practices, the following sections present two case studies of Vietnam and Myanmar, respectively, demonstrating the increasingly salient influence of the Chinese approach to cyber and data regulation abroad.

A. Vietnam's Cybersecurity Law

A typical example that manifests the influence of China's data governance approach is Vietnam's newly enacted cybersecurity law. Since its issuance in June 2018, Vietnam's cybersecurity law stipulated broad data localization requirements under vague and ambiguous terms.[2079] After several rounds of drafting, Vietnam finalized a decree (No. 53/2022/ND-CP) to implement the mandate of data localization in August 2022 (which took effect in October 2022).[2080] Based on the notion of "data sovereignty", Vietnam's data localization requirements aim to safeguard national security, social order and safety, and private rights and interests in cyberspace.[2081] As required by this regulation, domestic companies (including foreign-invested firms) must store personal data of service users and other user information ("regulated data")[2082] domestically, if they (i) provide services on telecommunication network, services on the Internet, or value-added digital services in Vietnam, and (ii) collect or process such data.[2083] As with its policy rationales, these broad and sweeping requirements echo and resemble China's horizontal data localization policies.[2084]

Meanwhile, the decree also applies data localization requirements extraterritorially. For foreign-based firms operating businesses in an enumerated digital service sector, the Ministry of Public Security may issue a decision to require them to comply with the data localization requirements and to establish a local branch in Vietnam, if they fail to comply with the authorities' requests to cooperate and deal with cybersecurity breaches that used their services.[2085] The data storage and local presence requirements must be completed within 12 months from the date of the decision.[2086] The local data storage must persist until the ending of the Vietnamese authorities' request (with a minimum storage time of 24 months), and the local presence shall be maintained until the foreign companies cease their operation (or provision of the enumerated services) in Vietnam.[2087] Similar to the Chinese approach, the extraterritorial effects of Vietnam's cybersecurity law are intended to

---

[2079] Taro Hirosawa et al., *Vietnam: New Official Guidance on Vietnam's Data Localization Requirements*, NISHIMURA & ASAHI ASIAN & DATA PROTECTION NEWSLETTER (August 22, 2022), https://www.lexology.com/library/detail.aspx?g=efe0bcfb-031b-4568-b9c1-fc375149a5f5 (Vietnam's cybersecurity law was effective in January 2019).
[2080] *Id.*
[2081] Loan Le & Paul Baker, *Vietnam: What Are The Data Localisation Implications of Viet Nam's Decree No. 53/2022 Relating to Cyberspace?*, MONDAQ (September 2, 2022), https://www.mondaq.com/security/1226892/what-are-the-data-localisation-implications-of-viet-nam39s-decree-no-532022-relating-to-cybersecurity.
[2082] Hirosawa et al., *supra* ("other user information" includes data generated by service users in Vietnam and data on their relationship (such as data of the friends and groups they have connected or interacted with)).
[2083] *Id.* (noting that this means that targeted domestic companies that were using overseas servers must store a copy of the regulated data in a Vietnam-based server).
[2084] Cybersecurity Law of the PRC, art. 37; Personal Information Protection Law of the PRC, art. 40 [PIPL].
[2085] Hirosawa et al., *supra* (the triggering conditions include (i) their services have been used to commit a violation of cybersecurity law, (ii) the authorities has informed them of such violations, and requested in writing for collaboration, prevention, investigation, and handling such violations, and (iii) they have failed to comply with such requests, or have obstructed the authorities' application of cybersecurity measures).
[2086] *Id.*
[2087] *Id.*

extend the government's "data sovereignty" to foreign-based data processing activities, in order to protect cybersecurity and national security.

Moreover, absent dedicated, specialized data protection authorities, the primary regulatory agency to implement Vietnam's cybersecurity law is the Ministry of Public Security. Under a cybersecurity-oriented mandate, this agency is vested by the decree with broad powers to censor and remove illegal online content,[2088] to request the disclosure of data relating to illegal activities in cyberspace, and to impose hefty sanctions on information system operators to protect national security, cybersecurity, and social order.[2089] As such, Vietnam's regulatory institution to spearhead online content control and implement data localization is reminiscent of China's super regulatory agency over cyberspace—the Cyberspace Administration of China (CAC).

B. Myanmar's Draft Cybersecurity Law

Similar to the case of Vietnam, the military regime of Myanmar issued a draft cybersecurity law in January 2022, drawing on China's Cybersecurity Law as a template in many important aspects. Under the broad mandate of cybersecurity, this law empowers the government to exercise extensive control over digital information, online content, and the digital economy. [2090] Institutionally, the draft law provides for the establishment of a cybersecurity steering committee, which is to be led by the military regime.[2091] As an overarching regulatory agency in the shape of the CAC, the steering committee is broadly mandated to police cybercrimes, implement cybersecurity policies, and lead regulatory actions and law enforcement relating to cybersecurity.[2092] In addition, the steering committee is vested with the authority to grant license to all digital platform service providers in Myanmar, conferring it with broad discretion to control market access for the relevant sectors.[2093]

Substantively, the draft law imposes stringent and comprehensive data localization requirements. All digital platform service providers are required to store their users' specified information (including "username, IP address, ID numbers, contact details and other user record") for three years from the users' first use of their services.[2094] For digital platform service providers having

---

[2088] Giang Thi Huong Tran et al., *Vietnam: Decree 53 Provides Long-Awaited Guidance on Implementation of Vietnam's Cybersecurity Law*, MONDAQ (Augsut 19, 2022), https://www.mondaq.com/security/1223282/decree-53-provides-long-awaited-%20guidance-on-implementation-of-vietnam39s-cybersecurity-law ("illegal online content" is vaguely defined as content that infringes on national security, propagandizes against the state, disrupts security or public order, or compromises economic order or socio-economic activities).

[2089] *Id.* (such sanctions include suspension or termination of information system operation and revocation of domain names.

[2090] Win Shwe Yi Htun, *Cyber Security Bill (Myanmar)*, NAGASHIMA OHNO & TSUNEMATSU NEWSLETTERS (February 2022), https://www.noandt.com/en/publications/publication20220225-3/ (noting that the objectives of the draft cybersecurity law are to "secure cyber systems, protect critical information infrastructure, and protect privacy of personal data of individuals, manage cyber-attacks, and support digital economy.").

[2091] *Id*.

[2092] *Id*.

[2093] Htun, *supra* (explaining that "digital platform service" is defined as "any over the top (OTT) service that can provide data, information, images, voice, text or video online by using cyber resources"; and that "digital platform service providers" include "businesses such as cloud services, media streaming, corporate online services, e-commerce services, ticketing services, e-banking services and any mobile services.").

[2094] *Id*.

more than 100,000 users in Myanmar, the draft law obliges them to store such data in a place designated by the authorities.[2095] As with China's Cybersecurity Law, the draft law establishes a separate framework for the protection of "critical information infrastructure" (CII),[2096] and obliges any information relating to CII to be stored at an authorized location, with the processing requirements to be stipulated by further regulations.[2097] CII operators are required to submit a cybersecurity report on a yearly basis.[2098] As such, the horizontal and broad requirements of data localization, the volume threshold triggering local storage obligations, and the prioritized protection for CIIs, bear close resemblance to the Chinese approach.

Moreover, the draft law grants the government with wide-ranging powers to request digital platform service providers to provide data necessary for national security and public interests without judicial oversight, and to investigate, monitor, and block any digital platform services.[2099] Meanwhile, the authorities are empowered to censor and remove online content under relatively vague and broad grounds.[2100] And the draft law also restricts the use of virtual private network (VPN) by requiring users to file for a registration from the state, while sanctioning any unauthorized use.[2101] If adopted, these requirements would bring Myanmar's cybersecurity regulations into closer alignment with China's data governance regime.

****

To be clear, the cybersecurity regulations of Vietnam and Myanmar did not replicate the exact rules and prescriptions of the PRC Cybersecurity Law verbatim, but rather designed their own formulations to implement data localization and strengthen sovereign control over data flows. However, these emerging cybersecurity regulations have obviously been influenced by China's internal data governance regime, since they drew on its normative rationales and emulated core substantive rules and regulatory institutions of the Chinese template (though adapted to the local context). In that sense, China's data regulation approach has shaped such developing countries' legal rules and institutional design to pursue cyber and data sovereignty, to regulate cybersecurity,

---

[2095] *Id*.
[2096] *Id.* (noting that the "CII" is broadly defined to include information infrastructure relating to "electronic government services…. finance and budgeting, water resources, transportation, communication, public health, electricity and energy, natural resources", as well as any such infrastructure classified for private use only).
[2097] Simon Makinson et al., *Update from on the Ground: Draft Cyber Security Law—Implications for Business in the ICT Sector in Myanmar*, ALLEN & OVERY PUBLICATIONS (March 2, 2021), https://www.allenovery.com/en-gb/global/news-and-insights/publications/update-from-on-the-ground-draft-cyber-security-law.
[2098] Htun, *supra*.
[2099] *Id.*
[2100] Dhevy Sivaprakasam et al., *Analysis: The Myanmar Junta's Cybersecurity Law Would Be a Disaster for Human Rights*, ACCESSNOW (January 27, 2022), https://www.accessnow.org/analysis-myanmar-cybersecurity-law/; Makinson et al, *supra* (noting that the government may take down online misinformation and disinformation, information "causing hate, disrupting the unity, stabilization and peace," and statements "against any existing law."); Andre Gan and Kenneth See, *Myanmar: The Introduction of Requirements for Digital Platform Service Providers*, BAKER MCKENZIE INSIGHTPLUS (January 28, 2022), https://insightplus.bakermckenzie.com/bm/data-technology/myanmar-the-introduction-of-requirements-for-digital-platform-service-providers#cntAnchor6 (noting that digital platform service providers are obliged to "prevent, remove, destroy or suspend certain information on its platform upon notification from (the authorities)."). The "obligation to *prevent*" may require digital platform service providers to proactively monitor and oversee sensitive online content provided through their services, entailing business "self-censorship" duties.
[2101] Sivaprakasam et al., *supra*.

and to address the relationship between state, market, and individuals, thus diffusing among their emerging digital governance frameworks.

In addition to these two notable examples, countries such as Kenya, Nigeria, Sierra Leone, Tanzania, Senegal also have enacted, or are considering, data localization measures modelled on the Chinese approach and centered around "cyber" and "data sovereignty".[2102]

III. "PUSH-AND-PULL" FACTORS UNDERLYING THIRD COUNTRIES' EMULATION

Having demonstrated the rising trend of policy diffusion, I now turn to a set of "push-and-pull" factors accounting for third countries' emulation of China's data governance approach. First, the Chinese government has been making increasingly assertive efforts to advocate for its vision of cyber and data governance at the international level, expanding its discursive influence in global digital governance. Second, since leading Chinese telecommunication firms and e-commerce platforms have been increasingly supplying digital infrastructures to overseas markets, this development enhances foreign governments' material capacity to control the digital realm, facilitating the diffusion of the Chinese regulatory approach.

Third, given its promise to achieve security, economic, and strategic goals (including political stability, cybersecurity, self-determined economic development, and a greater role of nation-states in global Internet governance), the Chinese approach to cyber and data governance generates normative appeal to foreign governments in some emerging markets, motivating them to imitate the PRC's norms, policies, and practices. Through these mechanisms and factors, China is empowered to exert indirect, yet important, influence on a growing number of developing countries, shaping their emerging data governance regimes with its own vision.

A. Chinese Government Advocating for Its Domestic Data Governance Approach Internationally

With the exponential growth of domestic Internet industry and its e-commerce market, China has become increasingly assertive in promoting its vision of "cyber" and "data sovereignty at the international sphere, in efforts to shape global digital governance discourses based on its domestic approach.[2103] At the *Politburo's 36th Collective Study Session* in October 2016, President Xi called on China to scale up its capacity to "set the agenda and make the rules for cyberspace at the international level", as a crucial step in making China a "cyber superpower".[2104] In a 2017 policy paper, the CAC explicitly recognized cyberspace as "a new arena of global governance", strategized to amplify China's influence in global Internet governance, and aimed to make its

[2102] Nigel Cory, *Writing the Rules: Redefining Norms of Global Digital Governance*, in CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 82, NATIONAL BUREAU FOR ASIAN RESEARCH (March 2022), https://www2.itif.org/2022-NBRsr97-china-digital-ambitions.pdf?_ga=2.204751381.480101597.1652729267-2102500758.1652729267#page=79.

[2103] Gao, *supra* (Data Regulation), 266; Cory, *supra* (Writing the Rules), 74. See Lu, *supra*.

[2104] *Central Communist Party's Politburo's 36th Collective Study Session on Implementing a Cyber Superpower Strategy*, October 9, 2016, http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm.

domestic approach part of the "international consensus".[2105] Under the *2021 Data Security Law*, China committed to actively participating in the formulation of international rules and standards on data security.[2106]

While China has been consistently promoting its vision of "cyber sovereignty" internationally, most recently, it has been increasingly pro-active in advancing its conception of "data sovereignty"—an extension of its Internet governance discourse—to influence global data governance.[2107] As part of the broader agenda to integrate its domestic norms into major institutions of global governance, the Chinese government is advocating for international acceptance of its domestic data governance norms, policies, and practices, providing an alternative to the U.S. and the EU's regulatory models.[2108] By advancing its cyber and data governance approach on the international stage, China strives to achieve three major strategic objectives.

First, domestic political and national security concerns have played an important role in shaping China's drive to become a global rule-maker for cyberspace. Since Beijing pretty much desires a secure and controllable domestic cyberspace to ensure regime security and social stability, that goal would be much easier to achieve if China could use its vision of cyber and data sovereignty to shape international standards of global cyber governance.[2109] By setting the norms and rules for transnational digital governance, China is able to boost the legitimacy of its domestic Internet and data governance, ward off unwanted foreign interference, reduce international criticism and demands for reform, and normalize governmental control over cyberspace and the digital sphere.[2110]

Second, the Chinese government is also motivated by its deep-seated concerns about national sovereignty.[2111] While China has deployed *domestic* laws, regulations, and policies to establish strong governmental control over cyber infrastructures and data flows hosted thereupon, the validity of its claims of cyber and data sovereignty at the *international* level eventually depends on the recognition of other sovereign entities, namely, nation-states and inter-governmental organizations. By making third countries subscribe to its preferred approach to digital governance, China can legitimize and consolidate its sovereignty claims over domestic cyberspace and its digital realm.

Third, global diffusion of the Chinese regulatory approach among third countries empowers China to expand its influence and soft power in the international arena, which are essential for making

---

[2105] *Implementing General Secretary Xi Jinping's Cyber Superpower Strategy and Advancing Cybersecurity and Informatization*, September 15, 2017, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.
[2106] Data Security Law of the PRC, art. 11 [DSL].
[2107] Erie and Streinz, *supra*, 4.
[2108] *Id*., 39; Cory, *supra* (*Writing the Rules*), 75, 78.
[2109] Simone McCarthy, *Could China's Strict Cyber Controls Gain International Acceptance?*, SCMP (September 30, 2019), https://www.scmp.com/news/china/diplomacy/article/3030758/could-chinas-strict-cyber-controls-gain-international.
[2110] Erie and Streinz, *supr*a, 4; Flonk, *supra*, 1927 (arguing that promoting online content control norms at the international level serve instrumental and ideational goals: "[n]otions of sovereignty and non-interference protect autocracies from unwanted interference in their regimes and prevent sanctions and demands for reform", and "autocrats are strongly motivated to develop norms that serve as an authoritative source of power, legitimizing authoritarian rule.").
[2111] McCarthy, *supra*.

Beijing a cyber superpower.[2112] By getting more foreign countries on board with its preferred norms, policies, and practices, China could establish its regulatory "sphere of influence", and become more influential in transnational rule-making for digital governance, countering the U.S.-promoted vision of a "free and open" Internet and unrestricted data flows.[2113]

To achieve these objectives, China has been deploying a multifaceted and coordinated strategy to proactively shape global Internet and data governance,[2114] acting as a rising "norm entrepreneur" to promote its vision of "cyber" and "data sovereignty" to other sovereign actors. This strategy is exemplified by four major aspects canvassed in this Section.

(A) Bracketing Security-Motivated Domestic Data Regulations in International Trade Negotiations

In international trade negotiations, China advances an alternative approach to the U.S.-designed template of digital trade rules, which prioritize free data flows and discipline data localization.[2115] Different from the U.S. position, the PRC refrains from using international trade agreements to export its domestic data governance approach to third countries.[2116] Rather, China has been consistently pushing for a self-judging "essential security interest" exception in international trade agreements.[2117] By carving out domestic data governance regime on grounds of national security and cybersecurity, China aims to reserve unfettered policy space for a state to exercise its desired level of control over internal and cross-border data flows in pursuit of "data sovereignty". While this position is largely defensive, China's proposals directly oppose U.S.-promoted new-generation PTA provisions designed to discipline its domestic Internet and data regulations. Further, they also present an alternative approach to regulating data flows in trade treaties for other third countries to follow, particularly emerging markets concerned about the widening "digital divide" between themselves and developed countries.

For instance, in the RCEP negotiations, China's forceful advocacy for self-judging exceptions to free data flow commitments and data localization prohibitions may impart the importance of "data sovereignty" to other ASEAN developing countries, which are gradually building out their domestic data governance frameworks.[2118] And China's status as the largest developing country and its growing trade relationships in the Asia-Pacific region would lend it greater influence,[2119] making foreign governments in emerging markets consider its proposals more seriously. Through active engagement with trade negotiations (especially those for mega-regional PTAs like the

---

[2112] *Id.* (quoting a Chinese cyber law professor Huang, Zhixiong: "It is clear that without meaningful involvement in international (rule-making), and without a strong voice in global cyber governance, then however strong you are domestically, you simply cannot become a cyber power.").
[2113] *Id.* See *China's Approach to Global* Governance, *supra*.
[2114] Cory, *supra* (*Writing the Rules*), 78.
[2115] For the U.S. template of PTA provisions, see e.g., TPP, arts. 14.11, 14.13; USMCA, arts. 19.11, 19.12.
[2116] Erie and Streinz, *supra*, 36 (noting that this is so, despite that China generally embraces international trade agreements as a foundation to regulate its international economic relations).
[2117] See RCEP, arts. 12.14(3), 12.15(3); *Joint Statement on Electronic Commerce, Communication from China*, INF/ECOM/32, May 9, 2019. See also *supra* chapter 5 ("China's Data Sovereignty"), section VI.A.(A)-(B).
[2118] *China's Evolving Data Governance Regime*, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (July 26, 2022), at 2, https://www.uscc.gov/research/chinas-evolving-data-governance-regime [USCC].
[2119] *Id.*

RCEP), China can spread its domestic data governance approach and its Internet discourse among developing countries with nascent data regulations, and educate them on its vision of "data sovereignty" and "cybersecurity", thus getting more like-minded countries on board.

(B) Promoting Its Preferred Norms in Regional and International Institutions of Global Governance

Different from its primarily defensive stance on data regulation in international trade negotiations, China has been actively promoting its vision of "cyber" and "data sovereignty" in regional and international institutions and venues of global governance. These include—most notably—the Shanghai Cooperation Organization (SCO), BRICS Grouping (Brazil, Russia, India, China, and South Africa), World Internet Conference (WIC), and the United Nations (U.N.).

As will be detailed later, the PRC deploys different strategies to promote its preferred norms, policies, and practices internationally, depending on the specific institutional context (e.g., membership homogeneity and the extent to which the targeted states are likely to internalize its approach). What has remained relatively consistent, yet, is that China advocates for a central role of the nation-state in regulating Internet infrastructure, online content, and data flows within its territory, citing the principles of "cyber" and "data sovereignty".[2120] In particular, under the notion of "cyber sovereignty", China advances a "*multilateral*" approach to global Internet governance,[2121] contending that cyberspace should be governed by an inter-governmental institution under U.N. auspices following the decision-making rule of "one country, one vote".[2122] At the core, this approach allows national governments to establish the rules and standards based on their sovereignty and on behalf of their citizens, with private-sector and non-state actors serving an advisory and ancillary role.[2123] This position stands in stark contrast with the U.S. promoted "*multistakeholder*" model, which enables business actors, the technical community, and civil

[2120] Erie and Streinz, *supra*, 40.

[2121] See *supra* chapter 5 ("China's Data Sovereignty"), section I.B. (outlining the third international dimension of "cyber sovereignty"). According to Lu, Wei, the former CAC head, China prefers a "multilateral" approach to global cyberspace governance, which refers to a state "making the rules based on the idea of the sovereignty of the nation-state representing its citizens"; while the U.S. promotes a "multi-stakeholder" approach, enabling all Internet stakeholders to jointly make the rules on an equal footing. See Wei Lu, *Cyber Sovereignty Must Rule Global Internet*, HUFFPOST (February 14, 2015), https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060; See also Elliott Zaagman, *Cyber Sovereignty and the PRC's Vision for Global Internet Governance,* 18(10) CHINA BRIEF JAMESTOWN FOUNDATION GLOBAL RESEARCH & ANALYSIS (June 5, 2018), https://jamestown.org/program/cyber-sovereignty-and-the-prcs-vision-for-global-internet-governance/.

[2122] Flonk, *supra*, 1931-32; Xinchuchu Gao, *An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model*, 57 INT'L SPECTATOR 15, 21 (2022) ("For China, the private-sector-led multi-stakeholder approach led to the cross-border, private, distributed architecture of the Internet, which poses a threat to state sovereignty…. The PRC's multilateral approach to cyber governance is thus primarily driven by sovereignty concerns.").

[2123] Anqi Wang, *Cyber Sovereignty and Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L. J. 395, 447 (2020) (noting that "[u]nder the multilateral model, the regulatory organization 'functions firmly in the hands of the governments in the committee' with advisory groups from technical, business, civil society, and international organization sectors that would 'advise and assist' them"). See Milton Mueller, *A United Nations Committee for Internet- Related Policies? A Fair Assessment,* INTERNET GOVERNANCE PROJECT (October 29, 2011), https://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for- internet-related-policies-a-fair-assessment/.

society to play a central role in global Internet governance, policymaking, and management, with the counseling and assistance of governments.[2124]

(a) Engaging with Like-Minded Countries in Regional Inter-State Organizations

(1) Socializing and Persuasion

In a regional inter-state organization or group where member states are relatively homogenous and more amenable to its influence and control, China often socializes and persuades like-minded countries to support its data governance approach through regulatory cooperation, capacity building efforts, and strategic framing. Exemplary cases in this regard are the SCO and BRICS.[2125]

Established in 2001, the original member states of the SCO included China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.[2126] Spearheaded by China and Russia, the SCO has built up its normative framework, initially focused on regional security issues to combat terrorism, separatism, and extremism (the "three evils").[2127] With common concerns over "color revolutions" and "interference from 'foreign hostile forces'", the SCO member states' cooperation largely revolved around maintaining regime stability as a theme.[2128] Since the conclusion of an *Agreement on Cooperation in the Field of International Information Security* in 2009, the SCO's international cooperation and policy coordination came to include a strong digital component.[2129] With President Xi attaching great importance to the SCO's joint work on information security,[2130] China played an important role in promoting member states' regulatory cooperation efforts on this matter, including exchanging expertise and best practices, providing technical assistance and training, conducting capacity-building events, and undertaking joint operations.[2131] For instance, the Regional Anti-Terrorist Structure (the SCO's standing body dedicated to combating "three evils") has coordinated two SCO Anti-Cyberterrorism Exercises in China in 2015 and 2017, respectively, building member states' capacity and experience to curb hostile forces' use of the Internet for terrorist, separatist and extremist purposes.[2132]

[2124] Wang, *supra* (*Cyber Sovereignty and Its Boldest*), 447 (noting that the ICANN model "gives more weight civil society and business groups for policy design and has governments perform the advisory role"); JEREMY MALCOLM, MULTI-STAKEHOLDER GOVERNANCE AND THE INTERNET GOVERNANCE FORUM 40-43 (2008).

[2125] Flonk, *supra*, 1935-38. As argued by Flonk, "[r]egional organizations are likely to be relatively homogenous, consisting of a limited number of often like-minded actors that usually share similar values and ideas, and thus being more likely to generate support for an emerging norm. Such a context creates opportunities for norm entrepreneurs to socialize other actors, for instance by referring to reputation, providing assistance and training, and naming and shaming outliers." See *id.*, 1929-30.

[2126] Shanghai Cooperation Organization ("SCO"), *Frequent Asked Questions*, http://eng.sectsco.org/docs/about/faq.html.

[2127] Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMMUNICATION 3835, 3841 (2018).

[2128] *Id.*

[2129] *Id.*, 3341-42.

[2130] Flonk, *supra*, 1935-36 (quoting President Xi Jinping's speech in September 2014 stating that information security cooperation showcased "the strong vitality of the SCO" and formed a solid foundation for the organization's future development).

[2131] *Id.*, 1936.

[2132] McKune and Ahmed, *supra*, 3842.

By facilitating information exchange in an iterative fashion, the SCO enables China (an influential member) to use its own domestic Internet governance policies and practices to inform, guide, and embolden other governments when studying and designing information control measures.[2133] Under the broad rubric of combating "three evils", China consistently emphasized the importance of regulating the Internet to prevent social protests and uprisings, and to protect ideological security and regime stability (broadly defined as "national security").[2134] Given that SCO members widely shared similar concerns about Internet-enabled campaigns deployed to overthrow incumbent regimes ("color revolutions"), China's repeated call for a peaceful cyberspace resonates relatively well with these countries in the region. This makes it easier for China to convince them of its framing of information technologies as a broad source of existential threats, potentially undermining a state's political, economic, and social security.[2135] As a result, this process of socialization and persuasion can lead SCO member states to accept the promoted norms, policies, and practices as legitimate and desirable, without critically questioning the validity or feasibility of their substance.[2136]

With such regional security cooperation mechanisms at work, SCO member states have increasingly coalesced around a common stance on maintaining governmental control over online content for regime security purposes.[2137] In a 2012 Declaration, the SCO heads of state agreed that they should build an information space based on the principles of respect for state sovereignty and non-interference in other countries' internal affairs.[2138] And SCO member states shared a consensus that the Internet must not be used to propagate terrorist, extremist, or separatist ideologies that endanger a state's national security,[2139] implicitly empowering governments to scrutinize online content for broadly defined security-oriented purposes.[2140] As such, to a large extent, China's vision of "cyber sovereignty" and its policies of Internet content control have been gradually internalized by other SCO members, and thus, are internationalized on a regional level.[2141]

Likewise, in the BRICS, member states have also been increasingly cooperating in information security work, as they intensified their efforts to exchange best practices and experiences, implement policy coordination against cybercrimes, and engage in capacity-building initiatives on

---

[2133] *Id.*, 3843.
[2134] Flonk, *supra*, 1940.
[2135] *Id.* (noting that "[t]his threat includes aspects such as the spread of radical and extremist ideas, the creation of an atmosphere of fear and panic in society, and the stirring up of social unrest.").
[2136] *Id.*, 1935, 1937.
[2137] *Id.*, 1937.
[2138] PRC Ministry of Foreign Affairs, *Declaration by the heads of state of the member states of the SCO on Building a Region of Lasting Peace and Common Prosperity*, June 7, 2012, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201206/t20120607_679336.html ("The member states will, on the basis of the principles of respect for state sovereignty and non-interference in other countries' internal affairs, work to build a peaceful, secure, fair and open information space.").
[2139] *Id.* ("The member states oppose the application of information and telecommunication technologies in a way that endangers their political, economic and social security and prevent the use of the Internet to propagate terrorism, extremism and separatism ideologies.").
[2140] The fact that what exactly constitutes online activities to "propagate terrorist, extremist, or separatist ideologies" is vague and ambiguous suggests that the governments' power to implement online content control may be broad and sweeping.
[2141] Flonk, *supra*, 1938; McKune and Ahmed, *supra*, 3841 (noting that the SCO has served as a first staging ground in the norm elaboration and diffusion process, which originally coalesced around "information security.")

this matter.[2142] Though their focus is less on developing substantive norms applicable to cyberspace, the BRICS countries paid close attention to cybersecurity issues, and repeatedly emphasized the need to build an intergovernmental institution of global Internet governance under U.N. auspices.[2143] Aligned with China's vision of "cyber sovereignty", they also explicitly recognized the applicability of principles of the U.N. Charter (including sovereign equality and non-interference in domestic affairs) to cyberspace.[2144]

(2) Sequencing in Policymaking

China resorted to the SCO forum to build regional coalitions for its Internet governance policies first, and then negotiated broader support at an international level, expanding small group consensus to a wider range of audiences.[2145] In this process, China aligned with Russia (another influential country spearheading the SCO) through normative collaborations, boosting their norm promotion efforts.[2146] Application of this policymaking strategy is exemplified by SCO member states' submissions on an *International Code of Conduct for Information Security* to the United Nations General Assembly (U.N.G.A.) in 2011 and 2015, respectively.[2147] Jointly led by China and Russia, the 2011 submission was supported by Tajikistan and Uzbekistan, and the 2015 submission endorsed by all SCO members.

Substantively, these submissions articulated China's conception of "cyber sovereignty" to a broader audience on the international stage. At the core, they underscored the "sovereign right" of a state to exercise authority over "Internet-related public policy issues".[2148] When regulating information security, such instruments required all states to comply with the U.N. Charter (that enshrines the principles of state sovereignty and political independence of a state), and to curb the spread of information inciting "three evils".[2149] In essence, these arguments highlighted China's preference to apply an absolute version of state sovereignty (unrestrained by human rights)[2150] from the physical sphere to cyberspace, justifying a nation-state's unfettered control over the

---

[2142] *Id.*, 1937. See e.g., BRICS, Ufa Declaration, July 9, 2015, para. 34, http://brics2022.mfa.gov.cn/eng/hywj/ODS/202203/t20220308_10649509.html.

[2143] Flonk, *supra*, 1938; Luca Belli, *Cybersecurity Convergence in the BRICS Countries*, CYBER DIGITAL EUROPE (Sept. 17, 2021), https://directionsblog.eu/cybersecurity-convergence-in-the-brics-countries/. See e.g., BRICS, Ufa Declaration, para. 34; BRICS, Fortaleza Declaration, July 15, 2014, paras. 48, 50; BRICS Leaders Xiamen Declaration, September 4, 2017, para. 56, http://brics.utoronto.ca/docs/170904-xiamen.html ("We consider the UN has a central role in developing universally accepted norms of responsible state behavior in the use of ICTs….")

[2144] BRICS, Ufa Declaration, para. 34 ("We emphasize the central importance of the principles of international law enshrined in the UN Charter, particularly the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states…."); BRICS Leaders Xiamen Declaration, para. 56.

[2145] Flonk, *supra*, 1942 (describing the sequencing strategy).

[2146] *Id.*, 1944.

[2147] Letter Dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, U.N. Doc. No. A/66/359, Sept. 14, 2011 ["2011 SCO Submission"]; Letter Dated 9 January 2015 from Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General, U.N. Doc. No. A/69/723, Jan. 13, 2015 ["2015 SCO Submission"]. The latter was based on the text of the former, though with minor revisions.

[2148] 2015 SCO Submission, 3.

[2149] *Id.*, 4-5.

[2150] McKune and Ahmed, *supra*, 3849 (noting that "It is well understood that China and Russia have subordinated human rights law to principles of sovereignty in their engagement with the international legal framework").

Internet and online activities within its territory to safeguard political stability, ideological interests, and national security. Meanwhile, the SCO submissions also advocated for "a prominent role" for the U.N. to develop "international legal norms for information security", calling for the establishment of a "multilateral" Internet governance system.[2151] This stance counters the "multistakeholder" system, which is largely dominated by the U.S. in the view of China.[2152]

While such SCO proposals did not received support by all U.N. member states, they are noted by the U.N. working group on information and communication technologies (the Group of Government Experts (GGE)) in its reports to the U.N.G.A.,[2153] evincing China-led norm development efforts in the international arena. In particular, countries that subscribe to a traditional, absolute conception of sovereignty may be more receptive to China's vision of cyber sovereignty, compared with those that conceptualize sovereignty as subordinated to human rights.[2154] Moreover, since India and Pakistan have joined the SCO as full member states and more countries obtained an observer status (or a dialogue partner status), China's notion of "cyber sovereignty" has been further expanded to wider member states, scaling up the diffusion of its preferred norms internationally.[2155] In this way, the SCO serves as a platform for China to disseminate its cyber governance norms, policies, and practices to the broader international community.[2156]

(b) Promoting Cyber Sovereignty at the World Internet Conference (the Wuzhen Process)

Another important venue for China to promote its vision of cyber sovereignty is the annual meetings of the World Internet Conference (WIC), co-hosted by the CAC and the government of Zhejiang Province (the birthplace of Alibaba) in Wuzhen since 2014.[2157] In 2022 alone, the WIC reportedly attracted more than 2,100 participants from over 120 countries and regions, including governmental officials, company executives, and industry experts from developed and developing economies.[2158] Past attendants include world leaders, representatives from global Internet governance institutions (such as the Internet Corporation for Assigned Names and Numbers (ICANN)), top executives of Apple, Facebook, Google, Amazon, and homegrown Chinese Internet giants, members of think tanks and the technical communities, Western media, as well as civil society.[2159] Aside from hosting high-tech exhibitions to promote the Chinese digital industry, the WIC also functions as an important discursive platform for the PRC government to advance its vision of Internet governance to an international audience.[2160]

[2151] 2015 SCO Submission, 5-6.
[2152] Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 120 (Dennis Broeders & Bibi van den Berg eds, 2020)
[2153] Flonk, *supra*, 1942.
[2154] Katharin Tai & Yuan Yi Zhu, *A Historical Explanation of Chinese Cybersovereignty*, 22 INT'L RELATIONS ASIA-PACIFIC 469, 493 (2022).
[2155] McKune and Ahmed, *supra*, 3843. See SCO FAQ, *supra*.
[2156] McKune and Ahmed, *supra*, 3842.
[2157] World Internet Conference (WIC), *Overview of WIC*, October 15, 2020, https://www.wuzhenwic.org/2020-10/15/c_547699.htm.
[2158] Yukun Liu, *Consensus Emerges on Shared Digital Future*, CHINA DAILY (Nov. 12, 2022), https://www.chinadaily.com.cn/a/202211/12/WS636ee857a3104917543294a8.html.
[2159] McKune and Ahmed, *supra*, 3845.
[2160] *Id.*, 3845-46 (noting that the WIC is "[p]art a diplomatic theatre and part a high-tech expo"). Pablo Hinojosa, *Wuzhen Summit: China Demonstrates Its Internet Vision*, APNIC (Nov. 26, 2014), https://blog.apnic.net/2014/11/26/wuzhen-summit-china-demonstrates-its-internet-vision/ (noting that the WIC

In December 2015, President Xi delivered a keynote speech at the opening ceremony of the second WIC,[2161] articulating China's discourse of Internet governance and cyber sovereignty. First, he explicitly called for "respect for cyber sovereignty", stating that the "principle of sovereign equality enshrined in the Charter of the United Nations" equally applies to cyberspace.[2162] On this basis, he urged respect for "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies", while condemning "cyber hegemony" and any "interference in other countries' internal affairs".[2163] In essence, this statement links China's vision of cyber sovereignty to well-established public international law principles of state sovereignty and non-interference in a state's domestic affairs, in order to anchor the former's normative foundation and boost its legitimacy and credibility. In this way, China strives to justify governments' territorial control over cyberspace, to legitimize their domestic management of various online activities (including filtering and censorship for political reasons), and to exclude any foreign intervention and influence from domestic cyber regulation, while countering the U.S.-promoted "free and open" view of the Internet.[2164]

Second, President Xi advanced a security-oriented framing of information technologies to convince other actors on the necessity of implementing sovereign control over the Internet. Stating that "[c]yber surveillance, cyber attack and cyber terrorism have become a global scourge", Xi emphasized the need to subject cyberspace to domestic laws to achieve "good order" in Internet governance, thereby maintaining cybersecurity for each country.[2165] Given that the WIC is attended by an array of non-like-minded public and private actors, this security framing is constructed to resonate with a broader liberal audience, to deflect criticism and controversy, and to circumvent concerns on infringement of online freedom of expression and human rights.[2166] Since cybercrime and cyberterrorism are widely seen as legitimate grounds for controlling online content by Western countries, they provide a common ground for China to rally international support for its preferred Internet governance norms, policies, and practices.[2167]

---

adopted a Davos style format, consisting of a trade-show and a conference, and that "influential Internet players, who indeed play an important role in shaping the Internet in China and abroad, delivered most of the content of the sessions.").

[2161] PRC Ministry of Foreign Affairs, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*, December 16, 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html [Xi's Remarks at the WIC].

[2162] *Id.* ("The principle of sovereign equality enshrined in the *Charter of the United Nations* is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace").

[2163] *Id.* See *President Xi Jinping's Views on the Internet*, CHINA DAILY (December 14, 2015), https://www.chinadaily.com.cn/china/2015-12/14/content_22706973.htm (quoting President Xi's speech at the 8th US-China Internet Industry Forum in Seattle in September 2015: "China proposes that all the countries institute its own Internet policy in line with its own national conditions….").

[2164] See McKune and Ahmed, *supra*, 3841 (noting that where two norms contest with each other, which norm prevails partly depends on its "relative compatibility or coherence with other prevailing norms").

[2165] Xi's Remarks at the WIC.

[2166] Flonk, *supra*, 1939.

[2167] *Id.* ("Since content control norms are not a dichotomy but a continuum on which the degree of control can vary, there are many grey areas where content control might be seen as legitimate…. Cybercrime and cyberterrorism relate to existential threats experienced by all members of the international community and are therefore used to mobilized support for content control norms.").

Meanwhile, though China securitized the framing of information technologies, it avoided the highly contestable issue of how much governmental control applied to cyberspace is legitimate.[2168] Given that liberal actors often have different perceptions over what constitutes appropriate control over the digital sphere from authoritarian regimes, this ambiguous stance makes "cyber sovereignty" a rather flexible norm capable of fitting within different contexts under different interpretations, further increasing its likelihood of policy diffusion.[2169]

Third, aside from the security framing, President Xi linked the notion of cybersecurity to digital development to increase the former's appeal to developing countries. As put by Xi, "[s]ecurity and development are like the two wings of a bird or the two wheels of a cart…. Security ensures development, and development is what security is aimed at."[2170] By framing cybersecurity as an indispensable precondition for promoting "orderly development" of digital industries, Xi further underscored the importance of controlling the Internet to safeguard cybersecurity. And China's example of developing a prosperous e-commerce market and an internationally competitive digital industry lends credence to Xi's arguments, emboldening emerging markets' confidence in following its vision of "cyber sovereignty".[2171]

(c) Advocating for Global Initiative on Data Security on the International Stage

More recently, China's norm promotion efforts increasingly centered on making international rules for data governance, exemplified by the "*Global Initiative on Data Security*" (GIDS) championing the PRC's vision of "data sovereignty".[2172] Officially announced by Chinese Foreign Minister Wang Yi at a high-level session of the China Internet Governance Forum in September 2020,[2173] GIDS proposed a framework to regulate data security and digital commerce, and has been widely seen as a strategic response to the U.S. "Clean Network" program (launched by the Trump administration to target Chinese technologies and exclude PRC tech firms from global Internet infrastructures).[2174] As put by Chinese Foreign Ministry spokesperson Zhao Lijian, GIDS aims at

---

[2168] *Id.*

[2169] *Id.*, 1940-41. However, for a critique on the lack of clarity of China's "cyber sovereignty" norm, see McKune and Ahmed, *supra*, 3847-48 ("Internet sovereignty is too amorphous to define and alert the international community and domestic audiences to the full scope of behavior that violates the norm, leaving interpretation of what constitutes interference with internal affairs entirely to government discretion.")

[2170] Xi's Remarks at the WIC.

[2171] See Lu, *supra* (touting China's achievements (including having the world's largest Internet market and competitive domestic Internet firms) as "testimony to the success of China's reform and opening up, of the development path chosen by the Chinese people, and the leadership of the Chinese communist party", and calling for respect for each country's cyber sovereignty and domestic Internet governance policies).

[2172] *Global Initiative on Data Security (Full Text)*, Sept. 8, 2020, http://www.gov.cn/xinwen/2020-09/08/content_5541579.htm [GIDS].

[2173] Paul Triolo and Graham Webster, *Translation: China Proposes 'Global Data Security Initiative'*, DIGICHINA (September 7, 2020), https://digichina.stanford.edu/work/translation-china-proposes-global-data-security-initiative/.

[2174] Chaeri Park, *Knowledge Base: China's 'Global Data Security Initiative'* 全球数据安全倡议, DIGICHINA (March 31, 2022), https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/. See U.S. Department of State, *The Clean Network*, https://2017-2021.state.gov/the-clean-network/index.html ("The Clean Network program is the Trump Administration's comprehensive approach to safeguarding the nation's assets including citizens' privacy and companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party.").

maintaining data security, promoting digital development, and "contributing Chinese wisdom to international rules-making on global data governance."[2175]

Substantively, the crux of GIDS is crystalized in eight tenets, founded on the recognition that each country has the responsibility and rights to secure and safeguard important data and personal data implicating national security, public security, economic security, and social stability.[2176] These tenets include China's proposed commitments on security of global supply chains,[2177] protection of CII and important data,[2178] local data storage, protection against foreign mass surveillance,[2179] and security of information technologies.[2180] In particular, GIDS seeks to export China's vision of "data sovereignty", subjecting the contestable issues of data storage and cross-border data transfers to a nation-state's domestic laws.

First, GIDS explicitly requires companies to strictly comply with local laws, and urges countries not to demand their domestic firms to store data generated or collected overseas within their own territory.[2181] Contrary to the U.S.-promoted prescription of free data flows across borders, this rule justifies a host state's measures to localize the storage of domestically originated data held by digital firms. Second, this instrument calls for "respect for the sovereignty, jurisdiction, and data security management rights of other countries", and demands countries not to "directly access data located in other countries from companies or individuals" without the permission of domestic laws,[2182] countering the application of the U.S. CLOUD Act. Aligned with the PRC Personal Information Protection Law's provision on cross-border data transfers for law enforcement purposes, GIDS emphasizes that such data transfers must be addressed through judicial assistance mechanisms or other mutual agreements to respect the jurisdiction and data security of a host country,[2183] in defense of its national data sovereignty.

Based on a state's territorial jurisdiction over digital facilities and infrastructures, these provisions establish the primacy of the government's "data sovereignty" in regulating cross-border data flows

---

[2175] *Whether Global Initiative of Data Security Targets the U.S. "Clean Network" Program, the Response by Zhao, Lijian*, CHINA ECONOMIC NET (September 9, 2020), http://www.ce.cn/xwzx/gnsz/gdxw/202009/09/t20200909_35706651.shtml.

[2176] GIDS, *supra*. Shannon Tiezzi, *China's Bid to Write the Global Rules on Data Security*, DIPLOMAT (September 10, 2020), https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/ (noting that these tenets reflect China's concerns (such as being cut off from access to Western technology and foreign digital firms), and intend to address concerns about China (eg., Chinese tech firms such as Huawei can install "backdoors", harvest data, or undermine information infrastructures at the behest of Beijing); and that they also evince data security risks brought by U.S. global digital surveillance, as suggested by Snowden revelations).

[2177] Park, *supra* ("treat data security objectively and rationally, and work to maintain open, secure, and stable global supply chains.").

[2178] *Id.* ("oppose the use of information technology to damage other countries' critical infrastructure or steal important data.").

[2179] *Id.* ("take measures to prevent and end personal information harms, and not abuse information technology to conduct large-scale surveillance of other countries or illegally collect personal information of citizens of other countries.").

[2180] *Id.* ("information technology product and service providers should not set up backdoors in their products or services to illegally obtain user data", and "information technology companies must not use users' dependence on their products to seek illegitimate gains.").

[2181] *Id.*

[2182] *Id.*

[2183] *Id.* See PIPL, art. 41.

originating from its own territory, subordinating private firms' commercial needs to domestic laws. Meanwhile, they also guard against foreign governments' unauthorized access to and control of those data, whether through domestic laws or intelligence surveillance,[2184] which are deemed a violation of the host state's territorial jurisdiction and national sovereignty over such data. As suggested by these provisions, China is now striving to solidify its domestic rules of data localization into international norms for data security, serving as a foundation for global data governance.[2185]

In addition to these tenets, China also proposed three principles to address challenges and risks relating to data security.[2186] Among them, the foremost principle is multilateralism, evincing China's push for a multilateral approach to global data governance.[2187] Aside from countering the U.S.'s unilateral approach behind its "Clean Network" program, China's promotion of multilateralism aligns with its longstanding preference for international rulemaking.[2188] While "multilateralism" sounds politically correct in many contexts, when dealing with Internet and data governance, this proposal attempts to move the decision-making authority over the digital sphere to greater sovereign control by nation-states, since governments often enjoy exclusive decision-making authority at a multilateral forum. By proposing a multilateral data governance model under the decision-making rule of "one country, one vote", this proposal shifts the momentum away from the private-sector-based "multistakeholder" approach to global cyber governance, which has long been dominated by Western-participation. Particularly, this multilateral approach marginalizes the participation of the private-sector and civil society,[2189] many of which oppose China's preferred norms of data localization and data sovereignty.

Since GIDS was announced, China has stepped up its diplomatic efforts to mobilize international support for this framework at bilateral, regional, and international venues. In the 2020 WIC, an official of the PRC Ministry of Foreign Affairs promoted GIDS as a "blueprint" for reaching international rules on data regulation, calling on other countries to formulate universal norms of cyber and data governance under the U.N. framework.[2190] In addition, China has advocated for GIDS at the China-Germany-EU leaders' meeting, the SCO, the BRICS Summit, the G20 Summit, World 5G Convention, 2021 World Digital Economy Forum Press Conference,[2191] China-Africa

[2184] Frequently Asked Questions, at 2, https://www.justice.gov/dag/page/file/1153466/download ("The CLOUD Act clarified that U.S. law requires that providers subject to U.S. jurisdiction disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data.").
[2185] Triolo and Webster, *supra* (quoting Wang, Yi: China hopes that its proposed GIDS can "provide a blueprint for the formation of international principles on data security, opening a global process.").
[2186] Park, *supra* (noting that these include "multilateralism", "secure development", and "fairness and justice").
[2187] *Id.* ("On the basis of widespread participation from all sides, we should reach global data security rules that reflect every country's wish and respect the interests of all sides.").
[2188] Park, *supra.*
[2189] See Justin Sherman, *China's War for Control of Global Internet Governance*, at 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4174453 (noting that while the multilateral approach to international cyberspace governance promoted by China also mentions "multi-party participation", under this approach only national governments have voting rights; in contrast, private actors, civil society, and other nonstate actors are only sources of "consultation", making them a secondary consideration at best.).
[2190] PRC Ministry of Foreign Affairs, *"Global Initiatives on Data Security" Infuses New Energy into Global Governance*, November 24, 2020, https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202011/t20201124_7668989.shtml.
[2191] Park, *supra.*

Internet Development and Cooperation Forum,[2192] as well as the U.N. Security Council.[2193] At the international level, GIDS has been endorsed by Tanzania, Pakistan, Russia, Ecuador, the Philippines, the Arab League, as well as ASEAN countries.[2194] In March 2021, China and the Arab League (consisting of 22 member states) signed the "*Sino-Arab Cooperation Initiative on Data Security*", essentially modeled on GIDS.[2195] Acclaimed by both parties as "an exemplary of developing countries participating in global governance", this joint initiative was intended to contribute to the development of international rules governing the digital realm.[2196]

(d) Norm Promotion in International Institutions of Global Governance

In addition to the foregoing norm promotion efforts, China has been increasingly proactive and assertive in advancing its vision of Internet and data governance in well-established global governance institutions, seeking to selectively reshape international processes to its preferred terms.[2197] These include not only private-sector-based Internet governance institutions—such as the ICANN and the Internet Engineering Task Force (IETF)—but also government-based multilateral institutions, including the U.N. and U.N. agency International Telecommunication Union (ITU).[2198] With respect to the former set of organizations, China adjusted its attitude from initial non-participation to increasingly active engagement in order to further its national interests, and thus, has gradually adapted to the multistakeholder-model of global Internet governance.[2199] Throughout this process, however, it has been consistently promoting a state-centered approach to Internet governance under the rationales of "cyber sovereignty", and, more recently, "data sovereignty".[2200]

What merits particular attention is the latter set of international institutions, as China is eager to make the U.N. and ITU play a more central role in global Internet and data governance.[2201] While

---

[2192] Ministry of Foreign Affairs, *Remarks by Assistant Foreign Minister Deng Li at China-Africa Internet Development and Cooperation Forum*, August 24, 2021, https://www.fmprc.gov.cn/eng/wjbxw/202108/t20210825_9134689.html ("China welcomes African countries' participation in…. the (GIDS).").

[2193] *Zhang Jun: Commonly Safeguarding Cybersecurity, and Jointly Protecting International Peace*, People's Net (June 30, 2021), http://world.people.com.cn/n1/2021/0630/c1002-32144907.html (at a cybersecurity-focused public meeting of the U.N. Security Council, China's U.N. ambassador Zhang, Jun referenced GIDS and its key concepts when articulating China's position).

[2194] Park, *supra.*

[2195] PRC Ministry of Foreign Affairs, *Sino-Arab Cooperation Initiative on Data Security*, March 29, 2021, https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202103/t20210329_9180823.shtml.

[2196] PRC Ministry of Foreign Affairs, *"Sino-Arab Cooperation Initiative on Data Security" Opens A New Chapter of Global Data Governance*, March 30, 2020, http://www.gov.cn/xinwen/2021-03/30/content_5596690.htm.

[2197] Erie and Streinz, *supra*, 39-42.

[2198] *Id.*; Jonathan E. Hillman, *A "China Model?" Beijing's Promotion of Alternative Global Norms and Standards*, TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (March 13, 2020), https://perma.cc/QZL3-GJ8U.

[2199] Erie and Streinz, *supra*, 35, 39-40; Gianluigi Negro, *A History of Chinese Global Internet Governance and its Relations with ITU and ICANN*, 13 CHINESE J. COMM. 104 (2020).

[2200] Erie and Streinz, *supra*, 40-41; Milton Mueller, *China and Global Internet Governance: A Tiger by the Tail*, in ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE 177 (Ronald Deibert et al., eds, 2011).

[2201] Cory, *supra* (*Writing the Rules*), 78-80. See eg., Information Office of the State Council of the PRC, *White Paper: The Internet in China*, June 8, 2010, http://www.china.org.cn/government/whitepaper/node_7093508.htm ("China

consistent with China's general approach to global governance,[2202] this stance is also due to important strategic considerations with respect to cyber rulemaking.

First, the U.N. venue provides national governments with exclusive voting rights, making it easier to marginalize private-sector advocacy groups and civil society that promote a "free and open" Internet.[2203] Second, the large membership of the U.N. not only boosts the legitimacy of its international rule-making,[2204] but also favors scale, enabling China to have "as many participants and proposals in as many forums as possible".[2205] Also, the U.N. can provide an important forum for negotiating an expansive cybercrime treaty favored by China and Russia.[2206] Third, in the U.N., China can use various incentives to get more like-minded countries to endorse its positions and proposals,[2207] expanding its allies to counter Western-dominated cyber governance models. Under the decision-making rule of a majority vote, the more countries that support the Chinese vision, the harder it is for other superpowers to turn their competing approaches into international standards.[2208]

Given these factors, China has been very proactive in promoting its broader view of Internet and data governance in the U.N. system, in an effort to legitimize its domestic policies and practices of online censorship and data localization and to integrate them into global standards.[2209]

In March 2017, China proposed an "*International Cyberspace Cooperation Strategy*" to the U.N. Conference on Disarmament, articulating its position and policy on global cyber governance.[2210]

---

holds that the role of the UN should be given full scope in international Internet administration. China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale.").

[2202] See Ministry of Foreign Affairs, *Position Paper of the PRC for the 77th Session of the United Nations General Assembly*, September 17, 2022, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wjzcs/202209/t20220917_10767412.html (emphasizing multilateralism as a cornerstone of the existing international order: "In the world, there is only one international system, i.e., the international system with the United Nations at its core. There is only one international order, i.e., the international order underpinned by international law. And there is only one set of rules, i.e., the basic norms governing international relations underpinned by the purposes and principles of the UN Charter.").

[2203] Cory, *supra* (*Writing the Rules*), 79.

[2204] Gao, *supra* (*An Attractive Alternative*), 23 (noting that "Beijing considers the UN 'the most legitimate global body' because all countries participate in it.").

[2205] Cory, *supra* (*Writing the Rules*), 79.

[2206] *Id.* Russia called for the development of an international treaty on cybercrime in the U.N. in 2010, but this proposal was rejected by the U.N, largely due to the opposition of the U.S. and the EU. See Mark Ballard, *UN Rejects International Cybercrime Treaty*, COMPUTER WEEKLY (April 20, 2010), https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty

[2207] Cory, *supra* (*Writing the Rules*), 79. Such incentives can include financial aids, development projects, or even the provision of covid vaccines. See McCarthy, *supra* ("support for China from countries that did not rank as major global powers but had ties or converging interests with Beijing could help China sell its vision of cyber governance in the UN arena.").

[2208] McCarthy, *supra.* (quoting a think tank analyst: "China favours a strong role for the United Nations in developing and managing a code of conduct in the governance of cyberspace, mainly because China is assessing that the bulk of UN member states would be more supportive [than rival states outside an international framework] of its view….").

[2209] See Hillman, *supra*, 7.

[2210] *Letter dated March 2017 from the Permanent Mission of the PRC, Addressed to the Secretary-General of the Conference on Disarmament: International Cyberspace Cooperation Strategy*, U.N. Doc. No. CD/2092, March 7,

Built on the SCO's U.N. submissions and President Xi's address at the WIC, this policy instrument voiced China's commitments to "establishing a just and coherent international cyberspace order" based on the principle of state sovereignty, emphasizing the rights of national governments to determine their domestic laws, regulations, and policies governing the Internet without any foreign interference.[2211] Further, speaking on behalf of the developing world, China highlighted insufficient representation of the Global South in global Internet governance, and advocated for a multilateral, open, and inclusive cyberspace governance system built on each country's equal participation and joint decision-making.[2212]

While such a proposed system would feature broad participation by all stakeholders, including states, international organizations, firms, technology associations, NGOs, and citizens,[2213] China emphasized that national governments should play a dominant role in leading global Internet governance and setting regulatory standards, particularly regarding public policy and security.[2214] Under the principle of "one country, one vote", developing countries would be endowed with greater decision-making authority at the proposed multilateral institution (due to their strength in numbers), thereby challenging Western-dominated global Internet governance processes.

In 2018, China, along with Russia and other like-minded countries, created a new U.N. working group on information and communication technologies (ICT)—the Open-Ended Working Group (OEWG)—as an alternative forum to the existing Group of Government Experts (GGC) that was more club-like and dominated by the U.S.[2215] Different from the GGC, the OEWG is open to all U.N. members to discuss and develop principles, norms, and rules about responsible state behaviors in cyberspace.[2216] In its submission to the OEWG in September 2019, China explicitly articulated its proposed principle of "State sovereignty in cyberspace":

> "It is widely endorsed by the international community that the principle of sovereignty applies in cyberspace. The Group should enrich and elaborate on the specification of the principle, thus laying solid foundation for the order in cyberspace. States should exercise jurisdiction over ICT infrastructure, resources as well as ICT-related activities within their territories. States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in cyberspace. States should refrain from using ICTs

---

2017, at 3, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/052/69/PDF/G1705269.pdf?OpenElement ["*International Cyberspace Cooperation Strategy*"].

[2211] *Id.*, 4, 6.

[2212] *Id.*, 5-6.

[2213] *Id.*, 5-6 (arguing that "[i]nternational cyberspace governance must insist upon multipartite participation, and a multilayered governance platform" should be built to enable all the relevant stakeholders to have a say).

[2214] *Id.*, 6-7 (advocating for "a multilateral, democratic and transparent global Internet governance system", where all states "have the right to participate in Internet governance on an equal footing", "ensuring that developing countries are better represented and able to have a say"). See Mueller, *supra*, 181 (noting that "when China uses the word 'democratic' in this context, it means one country, one vote. Its point of reference for 'democracy' is not the rights and interests of the individual citizen, but is equality among sovereign states."); see also Lu, *supra* (comparing the "multilateral" and "multi-stakeholder" approach).

[2215] Cory, *supra* (*Writing the Rules*), 79.

[2216] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, Seventy-Third Session (October 29, 2018), A/C.1/73/L.27/Rev.1, para. 5, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N18/342/13/PDF/N1834213.pdf?OpenElement.

> to interfere in internal affairs of other states and undermine their political, economic and social stability…."[2217]

Relatedly, China argued that the "principles enshrined in the UN Charter"—including "sovereign equality" and "non-intervention in the internal affairs of other states"—apply in cyberspace, serving as the "cornerstone of a just and equitable international order in cyberspace."[2218] In essence, China strives to export its domestic narrative of "cyber sovereignty" to the international level, and advocated for its adoption as a bedrock for universal principles applying across different countries. Different from the U.S.-promoted vision of a "free and open" Internet, China's approach focuses on a state's exclusive jurisdiction to control domestic ICT infrastructures and regulate online activities within its territory, in order to safeguard its perceived national security interests (including regime security, political stability, and ideological interests). If widely accepted at the international level, this vision of sovereignty would legitimize China's domestic Internet filtering and censoring practices in the international legal order, removing controversies and critiques surrounding its potential infringements of human rights (such as freedom to access the Internet, freedom of speech, and freedom of association).

In addition, China urged all U.N. member states to create a "*multilateral*" Internet governance system, and encouraged "a permanent and sustainable international process within the framework of the UN" to regulate cybersecurity.[2219] This echoes China's 2021 Position Paper on its cooperation with the U.N., stating that "China has all along supported the UN in playing a leading role in global governance on cyberspace".[2220] Again, these proposals and statements advance China's state-centered approach to cyber and data governance, countering the U.S.-led multistakeholder model that runs counter to its sovereignty-based vision. Also, they indicate China's ambition to expand the originally security-oriented discussions in the U.N. to a comprehensive agenda encompassing broader Internet and data governance issues, despite the latter being beyond the U.N.'s typical mandate.[2221] In so doing, China hopes to shift the center of cyberspace rulemaking processes to a government-based venue that is more amenable to its influence, vision, and interests.

B. Digital Silk Road: Chinese Technological Firms Acting as Infrastructural Agents

Alongside the Chinese government's diplomatic initiatives to promote cyber and data sovereignty, China also shapes transnational digital governance by exporting Chinese-built digital

---

[2217] China's Submissions to the OEWG, September 2019, https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf, para. II.(ii).
[2218] *Id.*, para. III.
[2219] *Id.*, paras. V, VI.
[2220] Ministry of Foreign Affairs of the PRC, *Position Paper on China's Cooperation with the United Nations*, October 22, 2021, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wjzcs/202110/t20211022_9609380.html. See also State Council Information Office of the PRC, *National Cybersecurity Strategy*, December 27, 2016, http://www.scio.gov.cn/xwfbh/xwbfbh/wqfbh/39595/41105/xgzc41111/Document/1660222/1660222.htm ("Support the United Nations to play a leading role, promote the formulation of international norms for cyberspace that are universally recognized by all sides…. Establish a multilateral, democratic and transparent international Internet governance system.").
[2221] See Cory, *supra* (*Writing the Rules*), 79. Note that the full name of the OEWG is the "Open-Ended Working Group on Developments in the Field of Information and Telecommunications *in the Context of International Security*" (emphasis added).

infrastructures and technologies to emerging markets, especially the participatory countries of its "Belt and Road Initiative" (BRI) (i.e., a massive state-led infrastructure project stretching Asia, Europe, Africa, and Latin America).[2222]

A crucial part of the BRI, China's "Digital Silk Road" (DSR) strives to promote, finance, and subsidize Chinese-built digital infrastructures to enhance digital connectivity and interoperability in the participatory countries,[2223] while boosting the internationalization and global market expansion of Chinese tech firms. As facilities for the collection, storage, processing, and transfers of data, these digital infrastructures include ICT networks (optical cables and wireless networks), national data centers (or data storage infrastructures), surveillance equipment (surveillance cameras, smart city sensors, facial recognition tools), and beyond.[2224] The rollout of the DSR is, to a large extent, intertwined with leading Chinese ICT and e-commerce companies' global expansion, fueled by the "Made in China 2025" plan (a nationwide industrial policy aimed at dominating high-tech sectors and developing an advanced manufacturing base).[2225] Both the DSR and Made in China 2025 dovetail with and are deployed to implement China's ambition of becoming a cyber superpower, empowering the PRC to maintain independent from critical foreign technologies,[2226] export Chinese technical standards internationally,[2227] and strengthen its influence in global digital governance.[2228]

Existing commentaries often focus on China's deployment of the DSR to set international technical standards for 5G telecommunication networks, surveillance equipment, artificial intelligence, cloud-computing, Internet-of-Things, and other cutting-edge technologies.[2229] What is relatively

---

[2222] Erie and Streinz, *supra*, 2. See James McBride & Andrew Chatzky, *China's Massive Belt and Road Initiative*, COUNCIL ON FOREIGN RELATIONS (January 28, 2020), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative (explaining China's "One Belt, Road" Initiative).

[2223] Erie and Streinz, *supra*, 2-4.

[2224] *Id.*, 6.

[2225] *Id.*, 5, 22. Adam Segal, *China's Alternative Cyber Governance Regime*, COUNCIL ON FOREIGN RELATIONS (March 13, 2020), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf (noting that under the DSR, "Chinese companies are searching for new markets and customers while the government is providing support (including loans and investments) in pursuit of economic, strategic and political goals."); See James McBride & Andrew Chatzky, *Is "Made in China 2025" A Threat to Global Trade?*, COUNCIL ON FOREIGN RELATIONS (May 13, 2019), https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade ("The program (Made in China 2025) aims to use government subsidies, mobilize state-owned enterprises, and pursue intellectual property acquisition to catch up with—and then surpass—Western technological prowess in advanced industries").

[2226] Richard Ghiasy & Rajeshwari Krishnamurthy, *China's Digital Silk Road and the Global Digital Order*, DIPLOMAT (April 13, 2021), https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

[2227] See Erie and Streinz, *supra*, 45 ("If Chinese technology companies build equipment according to a certain standard and export this equipment to other countries, the standards embedded in the products are exported as well."). And setting technical standards in emerging markets can cement Chinese firms' international competitive advantage against their competitors, while consolidating their global market shares.

[2228] Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, ATLANTIC (Jun 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

[2229] See e.g., Ghiasy and Krishnamurthy, *supra*; Alex He, *The Digital Silk Road and China's Influence on Standard Setting*, CIGI PAPER NO. 264 (April 4, 2022), https://www.cigionline.org/publications/the-digital-silk-road-and-chinas-influence-on-standard-setting/. See also Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty*, AEGIS PAPER SERIES NO. 1703, HOOVER INSTITUTION (June 2, 2017), at 13, https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf ("After China joined

underappreciated, however, is that along the DSR, Chinese tech firms' increasing supply of digital infrastructures to emerging markets also enables and facilitates host governments' practices and policies of online content control, surveillance of data, and localized data storage.

First, the establishment and operation of ICT networks and surveillance tools in developing countries with nascent (and often insufficient) data regulatory frameworks can provide host governments with more physical and technical means for online censorship, filtering, and blocking.[2230] For instance, powered by Huawei, the establishment of Pakistan Internet Exchange Point ensures that all data, whether domestically generated or transiting through the country, must be funneled through a single interface located in Islamabad,[2231] which can be used by the government as tools of online content control and surveillance.[2232] Under a political system that tends to prioritize national security and social stability over individuals' data privacy, this digital infrastructure may facilitate the government's emulation of Chinese Internet governance policies and practices, especially given that Pakistan's data protection laws are relatively thin and embryotic.[2233]

Second, as part of the DSR, Chinese companies, whether private or state-owned, have been proactively building national data centers in BRI countries and beyond, providing host governments with physical infrastructures to practise data localization policies. By way of example, Alibaba Cloud has built data centers in India, Indonesia, the Philippines, Thailand, ranking the first in the Asia-Pacific region for cloud computing services with a market share of over 25 percent.[2234] China Telecom Global, together with its partners, is vigorously expanding into BRI countries to build local data centers to host data storage systems and cloud computing services.[2235] ZTE has invested more than USD100 million to build the Bangladesh National Data Center,[2236] and Huawei has established national data centers in several BRI countries, such as Tanzania, Senegal, and Pakistan.[2237]

---

the World Trade Organization, it mounted a broad effort to define technology standards in software, hardware, and communication technologies. Chinese policymakers believed that controlling a standard ensured the capture of a large share of market value. Or as a phrase popular in the technology press in China put it, third-class companies make products, second-class companies develop technology, first-class companies set standards.").

[2230] Flonk, *supra*, 1944. See Segal, *supra* (*China's Alternative Cyber Governance Regime*) (noting that "[a]long with the hardware, Chinese firms also pass on training and techniques" required to use the exported infrastructure and technologies).

[2231] Erie and Streinz, *supra*, 81.

[2232] *State of Privacy Pakistan*, January 26, 2019, https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan.

[2233] See Erie and Streinz, *supra*, 75-76.

[2234] Wang Hai, *Alibaba Cloud Builds Five Data Centers in the Past Year to Speed Overseas Expansion*, YI CAI (June 1, 2022), https://www.yicaiglobal.com/news/alibaba-cloud-builds-five-data-centers-in-past-year-to-speed-overseas-expansion (As of June 1, 2022, Alibaba Cloud, the cloud computing arm of Alibaba Group Holding, has built five new overseas data centers in the past twelve months).

[2235] Andrew Kitson & Kenny Liew, *China Doubles Down on Its Digital Silk Road*, RECONNECTING ASIA (November 14, 2019), https://reconasia.csis.org/china-doubles-down-its-digital-silk-road/.

[2236] *ZTE Zhao Xianming: Building "One Belt, Road" National Information Highway*, SINA (May 22, 2017), https://tech.sina.com.cn/roll/2017-05-22/doc-ifyfkqwe0661865.shtml.

[2237] Cory, *supra* (Writing the Rules), 82-83; Dan Swinhoe, *Pakistani Government Opens Small New Data Center in Islamabad*, DCD (February 14, 2022), https://www.datacenterdynamics.com/en/news/pakistan-government-opens-small-new-data-center-in-islamabad/; *Huawei, ETPB Established Tier-3 Data Centre Facility*, ISLAMABAD POST (June 24, 2022), https://islamabadpost.com.pk/huawei-etpb-established-tier-3-data-centre-facility/.

Different from U.S. cloud service providers and digital firms that generally oppose local storage of data (largely due to the additional costs and complexities for global IT operations), leading Chinese tech firms often have no issues with foreign governments' mandate of data localization, and sometimes even advocate for localization policies.[2238] Given the widespread concerns over Chinese tech firms potentially sharing sensitive data collected abroad with the Chinese government, they seem to do this partly to earn trust for themselves, building confidence in data security and privacy protection.[2239] Meanwhile, they also saw an opportunity foregone by foreign cloud providers against data localization, and thus, strategized to seize that market share to boost their cloud computing service growth globally.[2240] Either way, with increasing market expansion and investments in emerging markets, Chinese firms' provision of physical infrastructures for local data storage would complement the PRC government's strategic goal to increase its influence and soft power in global data governance, facilitating recipient countries' convergence with China's data localization policies.

Third, along the DSR, China deploys commercial diplomacy not only to enhance market access for Chinese companies, but also to create support for its foreign policy and digital governance norms.[2241] To support Chinese ICT firms "going out", the Chinese government and state-owned financial institutions provide preferential loans and buyer credits to DSR host governments for Chinese-built digital infrastructures.[2242] While U.S. and European international development aid programmes often come with conditionality linked to democracy, human rights, transparency, and accountability, Chinese infrastructure funding is typically rendered without such strings attached.[2243] In contrast, alongside the deployment of state-backed ICT infrastructure development under the DSR, the PRC government advocates for its preferred norms and policies of cyber and data governance in its commercial diplomacy with BRI countries, which can undermine competing approaches advanced by the U.S. or the EU.

In lieu of formal treaties, China generally resorts to international soft-law instruments to coordinate its economic relationship with BRI countries, and has signed cooperative agreements with around sixteen countries to promote the DSR as of 2019.[2244] A notable example is the "*'Belt and Road'*

[2238] Cory, *supra* (Writing the Rules), 83 ("U.S. firms want to leverage the distributed nature of the internet to provide their services globally rather than build out unique IT systems for every market."). See eg., R Dinakaran, *Alibaba Ready to Comply with Govt Policy on Data Localisation*, BUSINESSLINE (December 6, 2021), https://www.thehindubusinessline.com/info-tech/alibaba-ready-to-comply-with-govt-policy-on-data-localisation/article24987381.ece (noting that Simon Hu, Alibaba Cloud's president, said the company insisted on data localization anywhere, whether in India or elsewhere: "It is our principle. Alibaba respects data security and privacy.").
[2239] Dinakaran, *supra* (while admitting the difficulty of building trust for Chinese firms, Simion Hu said Alibaba pushed for data localization to distinguish the company from other Chinese firms and to pitch for data security and privacy protection).
[2240] Surabhi Agarwal, *Alibaba Cloud Sees a Bright Lining in Data Localisation*, ECONOMIC TIMES (November 1, 2018), https://retail.economictimes.indiatimes.com/news/e-commerce/e-tailing/alibaba-cloud-sees-a-bright-lining-in-data-localisation/66454683 (according to a general manager of Alibaba Cloud India (which has set up two data centers in India), his company saw a big opportunity in the Indian government's push towards data localization, and had "a very aggressive growth plan for India" as a major market).
[2241] Segal, *supra* (Chinese Cyber Diplomacy), at 11.
[2242] *Id.*, 12.
[2243] *Id.*, at 11-12.
[2244] Erie and Streinz, *supra*, 62.

Digital Economy International Cooperation Initiative"—an overarching programmatic statement of the DSR, which was jointly launched by China, Laos, Saudi Arabia, Serbia, Thailand, Turkey, and the UAE at the fourth WIC in December 2017.[2245] While the substance of this initiative focuses on economic development aspects, there is a principle that underscores full respect for nation-state's cyber sovereignty and the importance of protecting cybersecurity, while calling on countries to build a multilateral Internet governance system.[2246] Another principle urges respect for each country's independent development paths,[2247] echoing the PRC-promoted sovereign right to self-determine a national approach to Internet and data governance to the exclusion of external interference. Reflective of China's diplomatic efforts to use its influence to foster international collaboration around its vision of digital governance, these statements may be instrumental in socializing and persuading BRI countries into the Chinese regulatory approach.

While China's diplomatic initiatives of norm promotion (generally or in the DSR context) spread the *normative element* of its vision of cyber and data sovereignty, Chinese firms' supply of digital infrastructures along the DSR furnishes the *capability element*. The latter enables and reinforces foreign governments' material capacity to regulate online content and practise data localization, which is required to achieve the normative principles of cyber and data sovereignty. Absent a robust domestic legal framework of data privacy protection, the provision of Chinese-built digital infrastructures in developing countries strengthens local governments' control over digital information and data flows within their own borders, catalyzing and facilitating the diffusion of Chinese cyber and data governance approach overseas.[2248]

C. The Normative Appeal of Cyber and Data Sovereignty

Beyond Beijing's proactive efforts of norm promotion and Chinese firms' facilitation, the spread of China's vision of cyber and data sovereignty can also be attributed to its inherent appeal for certain developing countries sharing more similarities to China than the West. Since its core tenets of governmental control and self-determined economic development promise to address important security, economic, and strategic concerns faced by numerous developing countries, China's approach to cyber and data governance generates significant appeal to a growing number of emerging markets and beyond.[2249]

[2245] Cyberspace Administration of China, "*One Belt, Road" Digital Economy International Cooperation Initiative*, May 11, 2018, http://www.cac.gov.cn/2018-05/11/c_1122775756.htm.
[2246] *Id.*, principle 14.
[2247] *Id.*, principle 13.
[2248] See Cory, *supra* (Writing the Rules) (noting that "[s]everal countries, including Kenya, Nigeria, Sierra Leone, and South Africa, have considered or enacted data localization policies and embraced notions of cyber sovereignty at the same time that Huawei and other Chinese firms were building data centers and expanding cloud services. Many countries are also considering using other China-related tech tools (e.g. surveillance) and digital regulations around content moderation (e.g., stifling free speech online)."); Sacks, *supra* ("Among other countries where China invests heavily, Nigeria has adopted measures requiring that consumer data be hosted in Nigeria, while Egypt has pending legislation that would mandate ride-sharing companies to store data in-country while also making it more accessible to authorities."). See also Segal, supra (Chinese Cyber Diplomacy), at 14 ("the presence on the ground of Chinese engineers, managers, and foreign ministry officials is likely to reinforce a natural tendency among developing countries, especially those with authoritarian governments, to embrace a vision of the Internet that puts states at the center.").
[2249] Erie and Streinz, *supra*, 85.

(A) Cybersecurity and National Security Concerns

China's vision of cyber and data sovereignty appeals to developing countries similarly concerned about cybersecurity and regime stability in the digital era. As the Snowden revelations broke trust for the U.S. as a global steward for free data flows across borders,[2250] national governments generally remain vigilant on U.S. mass surveillance of digitalized information. Relying on offshore cloud servers governed by foreign laws to store vast troves of domestically originated sensitive data risks creating "weaponized interdependence", and may translate into systemic vulnerabilities for a country, threatening data security, cybersecurity, and national security.[2251] Not only can the home country of such tech firms (e.g., the U.S.) surveil and control those data (the "panopticon effects"), but it also may leverage its jurisdiction over the infrastructure to cut off the supply of certain digital products and technologies to a targeted country as a tool of economic sanctions (the "chokepoint effects").[2252] In response, many countries see the policy of data localization as a viable solution to address such security concerns, though its effectiveness in practice is contested and controversial.[2253]

Further, as with China, many authoritarian regimes link the U.S.-led agenda of "free information flows" with the "Arab Spring", "color revolutions", and orchestrated efforts at regime change.[2254] Concerned with Internet-enabled campaigns deployed to fuel social unrest and undermine the perceived legitimacy of the incumbent political regime, such governments often embrace China's vision of cyber sovereignty as a normative justification to moderate, influence, and even control public discourses and online sentiment, thus cementing their regime stability.[2255] Domestically, they may welcome the notion of data sovereignty to justify their use of personal data as a means of social control to achieve social order,[2256] despite concerns of public surveillance encroaching on citizens' data privacy.

Even for democracies, the idea of strengthened governmental control over digital information and data flows also may seem an attractive proposal to safeguard cybersecurity and national security. As shown in the case of Cambridge Analytica, coordinated online misinformation campaigns launched by foreign intelligence agencies can heavily interfere with domestic presidential elections, undermining fundamental values and processes of democracy. Likewise, cyber-attacks exploiting the vulnerabilities of digital platforms, data centers, or CIIs may endanger social stability,

---

[2250] *Id.*, 88 (noting that while "U.S. technology companies have…. enjoyed a relatively high degree of freedom in their global operations…. They cannot escape the demands of their home jurisdiction", whether through the CLOUD Act or national security agencies' intelligence surveillance).
[2251] Henry Farrell & Abraham Newman, *Weaponized Globalization: Huawei and the Emerging Battler over 5G Networks*, 14 GLOBAL ASIA 8, 9-10 (2019) (discussing "panopticon effects" and "chokepoint effects").
[2252] *Id.*
[2253] For a view that questions the effects of data localization in protecting privacy and security, see Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. R. 677 (2015). See also Steward M. Patrick, *Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road*, COUNCIL ON FOREIGN RELATIONS (July 2, 2018), https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road (cautioning that Chinese tech firms may install backdoors in the digital infrastructure they installed, tap the data transmitted, and share those data with the Chinese government).
[2254] McKune and Ahmed, *supra*, 3841.
[2255] *Id.*, 3839 (arguing that "[r]egime stability is clearly at the forefront of (China's cyber) sovereignty agenda, and it is the most appealing promise of this norm for authoritarian developing countries.").
[2256] See Erie and Streinz, *supra*, 85.

economic security, and national security. In response, application of cyber sovereignty and data localization could reinforce national governments' monitoring of cyberspace, enabling them to better detect malicious cyber activities and strengthen the resilience of domestic information infrastructures. Also, it can facilitate local law enforcement and intelligence authorities' access to personal data required to tackle cybersecurity risks, improving the government's capacity to counter cyber-attacks and cybercrimes.

(B) Economic Interests and the Narrative of "Data Colonialism"

China's prosperous e-commerce market and internationally competitive digital industry make the Chinese approach to data governance alluring to many developing countries that desire to emulate its relatively successful transition to a digital economy. Through the transnational development project of DSR, the Chinese government and companies provide their own version of digital development to BRI countries and beyond, characterized by accessible digital infrastructures and governmental control of digital information.[2257] While maintaining state control over data flows conflicts with neoliberal prescription of free data flows, China's success in developing its own digital economy gives credence to the Chinese path of digital development, making many developing countries put faith in its promise to drive economic growth.[2258] Given that data has become an important resource for both economic development and machine learning algorithms,[2259] the idea of localizing data storage naturally attracts countries that want to leverage big data to develop their digital economy, foster technology innovation, and nurture domestic digital industry, following the development path set by China.

Further, China's vision of data sovereignty confronts and counterbalances the global dominance of U.S. digital multinationals, alluring countries intent on maintaining strategic autonomy in critical technologies and cultivating domestic champions in digital sectors. In particular, it echoes the narrative of "data colonialism", resonating with developing countries' prominent concerns of being economically dominated by U.S. big tech corporations as "digital colonizers".

Under classic account of colonialism, imperial powers extracted raw materials from their foreign colonies, and flooded the local markets with manufactured products in surplus, perpetuating their colonies' economic dependency and undermining the local industries.[2260] Likewise, the narrative of "data colonialism" also highlights such dynamics of structural dependency and entrenched inequality.[2261] When exporting digital services to "colonize" emerging markets, American digital giants siphon vast amounts of data from local users to extract commercial interests and develop their artificial intelligence algorithms, while accumulating profits, resources, and powers in the U.S.[2262] Overwhelmed by readily available digital products and technologies, developing countries

---

[2257] *Id.*, 89.
[2258] *Id.*
[2259] *Id.*, 85.
[2260] Michael Kwet, *Digital Colonialism Is Threatening the Global South*, ALJAZEERA (March 13, 2019), https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south/.
[2261] Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South*, 60 RACE AND CLASS 3 (2019).
[2262] Kwet, *supra* (ALJAZEERA); Danielle Coleman, *Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws*, 24 MICH. J. RACE & L. 416, 422-24 (2019).

not only find it difficult to develop a competitive domestic digital industry, but also are led to foster an economic and technological dependency on U.S. big tech, without obtaining a fair share of economic benefits created by their citizens' data.[2263] As a result, this narrative contends that today's global cyberspace landscape is characterized by a "center-periphery" structure. While U.S. digital giants largely monopolize proprietary digital infrastructures, machine learning algorithms, and key software applications to reap a lion's share of the burgeoning digital economy, developing countries are increasingly turned into "digital colonies" dominated by the former, with their people mainly serving as users and consumers.[2264]

Though labeled by pro-free-trade commentators as "ideologically-driven" and "protectionist",[2265] the narrative of "data colonialism" captures certain core concerns of many developing countries, and thus increasingly finds support in the Global South.[2266] In terms of transnational data regulation, many emerging markets are concerned that U.S.-promoted policy prescriptions of a "free and open" Internet and free data flows would further entrench the "digital divide" between themselves and the Global North (where multinational tech behemoths are typically domiciled), solidifying their status as "digital colonies" with their citizens' data being exploited beyond their control.[2267]

This is why countries such as India, Indonesia, and South Africa boycotted the Osaka Declaration of "Data Free Flow with Trust" at the close of the 2019 G20 Summit in Japan, arguing that the instrument did not reflect their national interests regarding data.[2268] Along the same lines, China frames the principle of data sovereignty and the policy of data localization as a valid solution to counter the U.S.'s "data hegemony" and American digital giants' global monopoly, and promotes an "inclusive, fair, and mutually beneficial" international economic order, whereby all countries can equally enjoy the benefits of their data resources.[2269]

[2263] Kwet, *supra* (ALJAZEERA); Jacquline Hicks, *Is the World's Data Being Affected by "Data Colonialism"?*, SILICONREPUBLIC (October 11, 2019), https://www.siliconrepublic.com/enterprise/data-colonialism-jacqueline-hicks-data-facebook.

[2264] See Yi Shen, *Cyber Sovereignty and the Governance of Global Cyberspace*, 1 CHIN. POLIT. SCI. REV. 81, 84-5 (2016). However, a notable exception to such dynamics is China: not only does China have home-grown Internet giants that are highly competitive at the international level, but it also has launched the DSR to finance and support BRI countries' construction of their own digital infrastructure. See *supra* Section III.B.

[2265] See eg., Cory and Dascoli, *supra*, 7 (arguing that the narrative of "data colonialism" is "ideologically driven, opposing capitalism, big businesses, the United States, and, in some cases, the use of data and digital technology itself").

[2266] Hicks, *supra*; Sally Adee, *The Global Internet is Disintegrating. What Comes Next?*, BBC (May 15, 2019), https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next (quoting Maria Farrell, a member of a UK-based Internet campaign organization Open Rights Group: "'Nations like Zimbabwe and Djibouti, and Uganda, they don't want to join an internet that's just a gateway for Google and Facebook' to colonise their digital spaces.").

[2267] Hicks, *supra* (noting that the widening disconnect between new sources of data (among developing countries) and the location of data centers (centered in the Global North) has led developing countries' accusations of "data colonization").

[2268] *Id.* See *G20 Osaka Leaders' Declaration*, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.

[2269] Yandong Gao, *Anti-Colonialism in the War on Data Sovereignty*, GLOBAL TIMES (February 16, 2022), https://www.globaltimes.cn/page/202202/1252383.shtml ("China must devote itself to defending its *data sovereignty* and oppose data exploitation (to protect itself from becoming the US' "data colonies")…. China should gradually change from strategic defense to taking the initiative and *advocating the concept of fair data use that benefits all*

Notably, China's discourse of data sovereignty appeals to developing countries' primary economic concerns, and presents the prescription of data localization as a straightforward and potent solution to a complex problem faced by the Global South. As a salient trend, many developing countries increasingly invoke the principle of data sovereignty to assert their jurisdiction over data (whether personal or not) generated within their territory, and to justify their compulsory requirements of domestic data storage. By demanding foreign digital firms to establish data centers, facilities, and permanent entities within their borders, developing countries strive to increase the amount of taxes imposed on the former, forge competitive advantages for domestic cloud computing companies, create more jobs for their citizens, stimulate ICT and energy investments, boost domestic digital industrialization, and climb up global value chain.[2270] In this way, these emerging markets aim to nurture and develop domestic digital sectors, and counter their economic and technological dependence on U.S. digital giants, while leveraging big data as a strategic resource to reshape their national competitive advantage in the digital era.

(C) Strategic Interests of Greater Participation in Global Internet Governance

China's vision of cyber sovereignty appeals to developing countries' desire to improve their representation and strengthen their decision-making authority in global Internet governance. Many "Global South" countries have long been reluctant to accept the multi-stakeholder model of global Internet governance, since they often perceive it as being dominated by the U.S.-led Western participation and consider that their voices are less powerful within such international processes.[2271] Under the multi-stakeholder model, the dominance of American civil society and tech companies with unmatched resources and technical advantages in designing Internet infrastructures largely aligns with and well serves U.S. interests, even if the U.S. government does not directly regulate the global Internet governance system, but rather favors inclusion and participation.[2272] This is why many developing countries are concerned that Internet standards and protocols would be controlled by U.S.-dominated global governance institutions (such as the

countries…. Restricting 'data export' is Beijing's only current means to fight Washington's data hegemony. In the long run, *China aims to promote a global view of data that is inclusive, mutually beneficial, and equal….* We must first *protect our own data security* so that we can have the strength to promote the establishment of *a fair international order on data*. In addition, China should work with the EU to *break the monopoly of the US internet giants*. *We cannot let data become a tool for the US to exploit other countries*. We should make data a resource for the happiness of people all over the world.") (emphasis added).

[2270] Hicks, *supra* (noting that many critics question the economic efficiency and technical viability of the data localization policy, initiatives to gauge the economic impact of localization often are "extremely partisan", used opaque methods, and potentially reflect bias; rather, "a 2018 study commissioned by Facebook found that its data centre spending in the US had created tens of thousands of jobs, supported renewable energy investments and contributed $5.8 billion to US GDP in just six years."); see *The Fact of Facebook's U.S. Data Center Fleet*, March 2018, https://baxtel.com/data-center/facebook/files/facebook_data_centers_2018.

[2271] Gao, *supra* (*An Attractive Alternative*), 17-18, 25; Segal, *supra* (Chinese Cyber Diplomacy) ("These countries often lack cybersecurity (and technological) expertise…. and see the multi-stakeholder process as expensive, opaque, and inefficient.").

[2272] Wang, *supra* (Cyber Sovereignty at Its Boldest), 404-5, 445 ("developing countries complained that the inclusiveness seems to only include dominant ICT carriers and other non-state sectors. These actors are usually composed of U.S. actors and cater to U.S. interests."); Eichensehr, *supra*, 347 ("Although the United States supports the multistakeholder model at least in part for freedom of expression reasons, the bottom-up governance model also serves U.S. interests because many of the nongovernmental voices that the model amplifies, including technology companies and nongovernmental actors, have ties to the United States or share its values.").

Internet Engineering Task Force).[2273] In addition, the Snowden revelations have further undermined the legitimacy of U.S.-dominated Internet governance processes.[2274]

With similar concerns,[2275] China advanced the principle of cyber sovereignty as an anti-monopolistic solution to challenge U.S. hegemony in global cyberspace governance, and instead advocated for a multilateral approach to ensure developing countries' equal participation and decision-making authority.[2276] While it is often criticized for top-down governmental control and restraining free speech, this multilateral approach repositions the decision-making authority of global Internet governance from private-sector and non-state actors back to national governments, in the belief that the Internet should be governed the same way as other traditional media.[2277] Under the "one-country-one-vote" rule, the multilateral approach would enable developing countries to enjoy greater policymaking authority than under the existing multi-stakeholder model, particularly given that many of them have weak or even no self-governed technical communities that can independently operate the Internet.[2278]

Meanwhile, under the rubric of cyber sovereignty, China called for "equitable distribution of the Internet's basic resources and joint management of critical information infrastructure" essential for the operation of cyberspace (such as root name servers),[2279] which are now highly concentrated in developed countries (especially the U.S.) despite that the majority of Internet users today are from developing countries.[2280] Overall, these Chinese proposals align with developing countries' strategic interests, and appeal to their salient concerns and discontent with the current Internet governance institutions, making China's view of cyber sovereignty more attractive to the Global South.

(D) Caveats

Before ending this section, it is worth noting three caveats here. First, while many states are drawn towards the Chinese approach to data governance, their claim of data sovereignty may be illusory if they primarily rely on Chinese companies to provide digital infrastructures and critical

[2273] Wang, *supra* (Cyber Sovereignty at Its Boldest), 445.
[2274] Gao, *supra* (*An Attractive Alternative*), 18 (noting that a number of developing countries "argue that the Snowden leaks prove that the US exploits mass surveillance data without any oversight, highlighting Washington's hypocritical behavior in cyberspace.").
[2275] *Id.*, 21-22 ("China's promotion of a multilateral approach reflects its desire to challenge the US hegemonic position in cyberspace. Beijing maintains that Washington has too much power in the current multi-stakeholder model and calls for the voice of new cyber powers to be heard in international Internet governance institutions, such as the ICANN and the Internet Governance Forum.").
[2276] See e.g., 2011 SCO Submission, art. II(7); *International Cyberspace Cooperation Strategy*, *supra*, 4-6. In this submission, China invoked U.N. Charter's principle of sovereign equality to contend that every country is entitled to participate in international Internet governance on an equal footing, and called for the establishment of a multilateral Internet governance system that better ensures developing countries' representation, equal participation, and voting rights. See *id*.
[2277] Wang, *supra* (Cyber Sovereignty at Its Boldest), 446-7.
[2278] *Id.*, 448.
[2279] *International Cyberspace Cooperation Strategy*, *supra*, 6.
[2280] Shen, *supra*, 85 ("13 top-level root name servers are governed by 3 companies, 3 government-related organizations, 3 universities and 1 non-profit private institution in the United States, 1 company and 1 private institution in Europe, and 1 Japanese organization respectively; and the ''hidden distribution server'' that sends root zone files to the 13 root name servers is owned and managed by VeriSign Inc. from the United States.").

technologies, since the latter (whether state-owned or private) are often under the influence of the party-state to varying degrees, enabling Beijing to access and control their data.[2281] To prevent and counterbalance "weaponized interdependence", a country needs to retain its control over domestic digital infrastructures to effectively govern the data hosted thereupon.[2282] Eventually, the degree of "data sovereignty" enjoyed by a developing country may depend on the availability of alternative digital infrastructures, its economic power and technological capacity, as well as the effectiveness of its domestic legal system of data protection.[2283] For this reason, the fact that many third countries increasingly emulate China's data governance approach (i.e., data localization measures on the books) is not inherently conflictual with China's (potential) ability to access foreign-stored data (*de facto* asymmetrical control) through Chinese firms that supply, operate, and manage digital infrastructures and technologies overseas.

Second, it is unclear to what degree developing countries can successfully replicate China's path of digital development, since China's economic success largely depends on its distinctive features that many states do not share—most notably, its huge population and enormous domestic market.[2284] In short, despite the appeal of cyber and data sovereignty as promoted by China, it is quite another thing as to whether, and to what extent, this approach to data governance and digital development can deliver its promise as expected.

Third, a state's emulation of China's governmental control and censorship of domestic and cross-border data flows risks undermining the Internet's potential to facilitate international interconnectedness, and may infringe on their citizens' individual rights and civil liberties.[2285] Assertion of cyber and data sovereignty can come at a cost of creating such negative externalities.

However, notwithstanding these caveats, tradeoffs, and drawbacks, they might not prevent many developing countries from imitating China's sovereignty-oriented policy prescriptions. This is because the underlying motivation is to establish governmental control over data flows for the aforementioned security, economic, and political purposes, driving the diffusion of China's approach to data governance.[2286] Further, the PRC's success in exerting considerable governmental control over data flows and developing a burgeoning digital economy would embolden recipient countries' confidence in modeling their nascent regulatory frameworks on the

[2281] Erie and Streinz, *supra*, 5, 81-82 (arguing that "Chinese companies that are building and operating the digital infrastructure are inextricably intertwined with the party-state and may share data with Beijing when requested to do so."); See Mark Wu, *The "China, Inc." Challenge to Global Trade Governance*, 57 HARV. INT'L L. J. 261, 269-84 (2016) (detailing the "uniqueness of China's Economic Structure" that empowers the Chinese party-state to maintain varying degrees of control over Chinese state-owned and private enterprises: "state assets oversight, financial sector organization, role of state planning, forms of corporate networks, political party involvement, and state-private sector linkages.").
[2282] Erie and Streinz, *supra*, 5, 87 (arguing that "weaponized interdependence is a function of uneven control over digital infrastructures.").
[2283] *Id.*, 87.
[2284] *Id.*, 90 (noting that China's massive consumer base "makes it feasible to develop a digital ecosystem that aspires towards a relatively high degree of independence from foreign companies and subjects those that are allowed to operate within China to a regulatory straightjacket."); Henry Gao, *Data Regulation with Chinese Characteristics*, in BIG DATA AND GLOBAL TRADE LAW 245, 266-67 (Mira Burri ed., 2021).
[2285] Erie and Streinz, *supra*, 85.
[2286] *Id.*

Chinese approach, lending credence to the latter's promise to solve their security, economic, and strategic challenges.

D. Carving Out an International Trade Exception for Inbound Data Flows

While China's primary approach to transnational digital governance is to shape the emerging international standards based on its domestic approach to data governance, it also attempts to carve out an exception in international trade agreements to accommodate its burgeoning economic interests, thus increasingly accessing foreign-originated data for commercialization.

As Chinese tech firms arise as crucial suppliers of digital infrastructures in emerging markets and beyond, they increasingly collect and process a myriad of overseas data, many of which are valuable personal data. As an important input to train machine learning algorithms, such data can serve as precious resources for Chinese companies to improve their artificial intelligence systems and extract economic value, benefiting China's domestic digital industry. For example, the widespread installment and daily operation of made-in-China surveillance equipment (such as security cameras and sensors) in DSR countries have been harvesting a magnitude of non-Chinese personal data, which can unleash enormous potential in expanding the capacity of Chinese facial recognition technologies.[2287] However, ironically, host governments' adoption of data localization measures may impede cross-border data flows, undercutting China's growing economic interests in accessing and commercializing such data.

To address this dilemma, China recently strives to selectively reshape U.S. promoted international trade-based approach to regulate cross-border data flows. In November 2020, China acceded to the RCEP that contains a binding free data transfer provision designed by the U.S. to facilitate *inbound* personal data flows, but pushed through a self-judging essential security interest exception, which can be invoked to justify and exempt its domestic security-motivated data localization measures restricting data *export*.[2288] In so doing, China seeks to safeguard dominant national security interests on the home front, while accommodating its rising economic interests abroad.

In a similar vein, China have made formal requests to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA) in 2021.[2289] On the one hand, it aspires to embrace these two treaties' robust provisions on free data flows to enable foreign-based Chinese firms to transfer data harvested overseas back to the Chinese market.[2290] On the other hand, China can invoke the self-judging

---

[2287] Lynsey Chutel, *China Is Exporting Facial Recognition Software to Africa, Expanding Its Vast Database*, QUARTZ (May 25, 2018), https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-. ("Zimbabwe may be giving away valuable data as Chinese AI technologists stand to benefit from access to a database of millions of Zimbabwean faces Harare will share with CloudWalk…. The machine learning needed to expand the technology's capability would require sufficient data…. Rolling out the technology in a majority black population will allow CloudWalk to more clearly identify other ethnicities, getting ahead of US and European developers."); Anna Gross and Madhumita Murgia, *China Shows Its Dominance in Surveillance Technology*, FINANCIAL TIMES (December 27, 2019), https://www.ft.com/content/b34d8ff8-21b4-11ea-92da-f0c92e957a96.

[2288] See *supra* chapter 5 ("China's Data Sovereignty"), section VI.A.(B).

[2289] State Council Information Office of the PRC, *China to Advance Efforts in Joining CPTPP, DEPA Trade Pacts*, Press Release (May 27, 2022), http://english.scio.gov.cn/pressroom/2022-05/27/content_78239741.htm.

[2290] See CPTPP, art. 14.11(2).

essential security exception of the CPTPP to immunise its domestic data localization measures from international adjudication.[2291] And while the DEPA contains no such an exception, its provisions are not subject to mandatory international dispute settlement,[2292] ameliorating China's concerns of being challenged against its domestic data regulatory approach. Further, for both treaties, without the presence of the U.S. as a rival superpower, China can become more assertive in shaping these trade rules based on its own vision, interpretation, and interests.

That being said, the Chinese government might find it increasingly challenging to coordinate its norm promotion efforts and an international trade exception as such. Given the widely perceived intertwined relationship between Chinese firms and the party-state, as well as China's geopolitical tensions with some neighboring countries, certain foreign governments may invoke self-judging security-oriented exception to restrict or ban data flows to China, citing cyber sovereignty and national security concerns over Beijing's unauthorized access to those data (whether through intelligence surveillance or domestic institutions).[2293] As such, its promoted norms of cyber and data sovereignty could backfire against Chinese digital firms operating in foreign markets. In response, China may resort to commercial diplomacy and foreign policy tools (such as lending, foreign assistance, capacity building initiatives) to de-escalate such tensions, foster goodwill, and build trust for Chinese enterprises, paving the way to facilitate inbound data flows. Alternatively, it also can deploy tit-for-tat economic sanctions (i.e., tariffs) to compel such a country to back down, invoking the PIPL and DSL's mandates to enforce countermeasures against perceived foreign discriminatory or restrictive measures.[2294]

In short, by repurposing the provisions of trade treaties, China attempts to create a version of "Chinese exceptionalism" to cross-border data flows. Thus, even if China's accession to the CPTPP and DEPA are successful, their data transfer commitments are unlikely to result in a paradigm shift in China's domestic data regulations and policies—nor will they change the PRC's international advocacy for its cyber and data sovereignty. Rather, China's selective reshaping may recalibrate and adapt these digital trade rules to suit its strategic national interests, creating an international trade exception to the global diffusion of its data governance approach.

IV. CONCLUSION

[2291] See CPTPP, art. 29.2(b).
[2292] See DEPA, https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf.
[2293] See Siladitya Ray, *India Bans TikTok, 58 Other Chinese Apps, Citing Security Concerns*, FORBES (June 29, 2020), https://www.forbes.com/sites/siladityaray/2020/06/29/india-bans-tiktok-58-other-chinese-apps-citing-security-concerns/?sh=2c82f1fb7e60 (noting that the Indian government has blocked access to 59 Chinese smartphone apps (including TikTok and WeChat), raising cyber sovereignty and national security concerns that those apps were "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers" located outside India).
[2294] PIPL, art. 43; DSL, art. 26. For an example of China's use of economic sanctions as foreign diplomacy tools, see *China Hits Australian Industries with Economic Sanctions Amid Souring Ties,* Business Standard (July 9, 2021), https://www.business-standard.com/article/international/china-hits-australian-industries-with-economic-sanctions-amid-souring-ties-121070900082_1.html ("China has hit Australian industries with economic sanctions as part of punishment over Canberra's criticism of Beijing blocking investigations into the origin of the COVID-19 pandemic and restrictions on Huawei Technologies…. imposing hefty tariffs on Australian barley and wine exports while throwing up barriers to several other products including timber, lobster, and coal.").

As a regulatory approach in parallel to the U.S. and the EU models, China's data governance norms, policies, and practices have been increasingly emulated by like-minded third countries amenable to its international influence, contributing to Beijing's emerging regulatory "sphere of influence" internationally. Importantly, an increasing number of developing countries have been adopting, or are considering, domestic regulations mirroring core elements of the Chinese data governance approach—including the principles of "cyber" and "data sovereignty", the practices of online content control, and the measures to localize data storage for cybersecurity and national security purposes. Focused on this notable, yet relatively understudied, phenomenon of "policy diffusion", this paper canvasses and systemizes the mechanisms and factors driving such recipient countries' imitation of the Chinese regulatory approach, accounting for their increasing convergence with the Chinese data governance regime.

First, with a bold ambition to become a global rule-maker (instead of a rule-taker), the Chinese government has been assertively promoting its vision, norms, and policies of cyber and data governance at regional and international venues and institutions, including the SCO, BRCIS Grouping, WIC, U.N., and ITU. Such discursive efforts have been multifaceted, coordinated, and proactive, largely driven by the political and strategic motivations to increase legitimacy of China's domestic approach, to reduce international criticism and demands for reform, and to increase its international influence and soft power in transnational digital governance.

At the core, China's discourses frame cyber and data sovereignty as a natural extension of well-entrenched international law principles of state sovereignty and non-inference from the physical realm to information space, and promote these norms as particularly benefiting developing countries in internal and global cyberspace governance. Through mixed promotion strategies of socialization, persuasion, and sequencing, China tailors its advocacy efforts to suit the specific institutional context, making its position and proposals resonate with different categories of audiences at regional and international levels.

Second, in international trade negotiations, China actively pushed for self-judging national-security-based exceptions to subordinate U.S.-promoted data transfer provisions to a state's sovereign prerogatives in defense of its perceived security and strategic interests. Given China's status as a leading developing country and its economic influence, its position and proposals may educate developing countries on importance of "cyber" and "data sovereignty", setting a notable example for them to study and emulate in their own trade negotiations. Such rulemaking efforts also exemplify China's selective reshaping of U.S.-designed regulatory template targeting Chinese data regulations, thus recalibrating such rules to suit its shifting national interests.

Third, with the unfolding DSR, Chinese tech firms have been increasingly supplying digital infrastructures to emerging markets, diffusing the normative influence of the PRC's regulatory approach abroad. Since many of the exported physical infrastructures include local data centers, Internet infrastructures, surveillance tools, and smart city projects, this process in effect enables and facilitates foreign governments' implementation of data localization, online content control, and public surveillance of data—especially for authoritarian developing countries with nascent, weak, or even non-existent data protection laws.

Fourth, due to their inherent ideational appeal, the PRC's vision of "cyber" and "data sovereignty" increasingly gains traction with developing countries sharing same incentives and grappling with similar policy challenges with China. Concerned with salient cybersecurity threats, the widening "digital gap" with the Global North, as well as underrepresentation and marginalization in global Internet governance, these countries are drawn to China's approach to cyber and data governance, whose policy and legal prescriptions promise a powerful solution to address their shared security, economic, and strategic problems.

As a set of "pull-and-push" factors exclusive of coercion, the PRC's proactive norm promotion efforts at the international level, its strategic digital trade rulemaking, Chinese firms' export of digital infrastructures along the DSR, and the ideational power of China's vision have collectively contributed to the global diffusion of the Chinese data governance approach among third countries. Though China does not compel its trading partners to adopt its regulatory approach in trade treaties or international agreements, the core tenets and principles of its internal data governance regime have been increasingly emulated by governments of developing countries in their domestic laws, empowering the PRC to solidify and export its domestic norms, policies, and practices into the emerging international standards.

Chapter 7

Concluding Remarks

Focused on transnational regulation of cross-border personal data transfers for commercial purposes, this PHD project has delved into the creation, development, and diffusion of three distinct regulatory approaches, each of which has been advanced by the U.S., the EU, and China, respectively. Specifically, it addressed three major research questions: (i) what are the Big Three's conceptualizations of personal data with respect to this issue-area, which can generate significant normative implications; (ii) why and how these great powers are deploying competitive lawmaking strategies to shape the rulemaking over cross-border data flows in the transnational regime complex; and (iii) how their preferred regulatory approaches are increasingly influencing third countries, shaping the latter's emerging data governance frameworks with their own visions and preferences. This chapter summarizes the core arguments and major findings of this project (Sections I to III), and ends with a discussion on the Big Three's implications for transnational data governance (Section IV).

Table of Contents

I. THREE DIFFERENT CONCEPTUALIZATIONS OF PERSONAL DATA AND THE NORMATIVE IMPLICATIONS 335

A. Three Major Conceptualizations 335

B. Switching and Adaptations 336

II. COMPETITIVE LAWMAKING STRATEGIES TO SHAPE THE GOVERNING RULES IN THE TRANSNATIONAL REGIME COMPLEX 337

A. The U.S. 338

B. The EU 338

C. China 339

III. DIFFUSION OF THE BIG THREE'S REGULATORY APPROACHES IN THIRD COUNTRIES: THREE EMERGING REGULATORY "SPHERES OF INFLUENCE" 340

A. The U.S. 340

B. The EU 341

C. China 342

IV. IMPLICATIONS OF THE REGIME COMPLEXITY FOR TRANSNATIONAL DATA GOVERNANCE 343

A. The Western Blocks vs. The Eastern Block? 343

B. Legal Fragmentations, Regulatory Barriers, and Transaction Costs 345

C. Divergent Interests of the Big Three, Long-Persistent Regime Complexity 347

I. THREE DIFFERENT CONCEPTUALIZATIONS OF PERSONAL DATA AND THE NORMATIVE IMPLICATIONS

Focused on the Big Three's major regulatory approaches to cross-border personal data transfers, this thesis unpacked three primary (yet not mutually exclusive) conceptualizations of personal data, and discussed their normative implications for the regulatory design to govern this contentious issue-area.

A. Three Major Conceptualizations

Aligned with their respective policy preferences, the U.S., the EU, and China adopt different primary conceptualizations of personal data—as a factor of production, an embodiment of fundamental rights, and an element of national security, respectively. Emphasizing a particular attribute of personal data and sidelining others, such conceptual framings differ in what they characterize as the most prominent interests at stake, in how they organize the underlying relationship between individuals, their data, and the governments, and in what they frame as the most important policy objectives for regulatory interventions. Embedded in different ideologies and philosophies, these conceptualizations contain irreducible normative components—ranging from neoliberalism to human rights and to state sovereignty—making the regulatory contestations over cross-border data flows unable to be readily addressed. Moreover, different conceptual framings mandate and justify competing legal paradigms to regulate this issue-area, which diverge in their basic logics, normative justifications, policy priorities, as well as legal and regulatory solutions.

Framing personal data as an intangible factor of production, the U.S.'s primarily economic conceptualization of personal data justifies a market-oriented approach to regulate cross-border data flows. Focused on maximizing economic efficiency and minimizing transaction costs, this regulatory approach encapsulates the policy prescriptions of neo-liberalism, including trade liberalization, deregulation, and business self-regulation. Through this analytical lens, the primary policy goals for a state's regulatory interventions should be to maximize the economic value of data, to enhance the prosperity achieved by the data-driven economy, and to spur the growth of cutting-edge technologies that are heavily reliant on data (especially personal data).

Treating personal data as an embodiment of fundamental rights, the EU's primarily rights-oriented conceptualization justifies a fundamental rights paradigm to regulate cross-border data flows. Different from an economic approach, this paradigm prioritizes high-standard data privacy protection, and treats that as a core criterion for allowing outbound personal data flows. From the perspective of this paradigm, the market mechanisms (i.e., industry self-regulation) are not sufficient—instead, the regulatory state should step in to implement a comprehensive and robust data protection regime, in order to adequately safeguard individuals' fundamental rights as a normative priority.

Unlike the prevailing U.S. and European conceptual framings, China's primarily security-focused conceptualization regards personal data as an indispensable component undergirding a country's

national security and data sovereignty. Since nowadays data plays a prime role in economic development, technological advancement, social governance, and national defence, data security can increasingly implicate a country's national security. Among various interests underlying data flows, this conceptualization underscores the protection of national security as a normative priority. To that end, a nation-state should construct and implement a security-oriented set of domestic laws, institutions, and processes to establish the regulatory standards for intra-country and cross-border data flows.

B. Switching and Adaptations

To be clear, these dominant conceptualizations are not mutually exclusive to each other. To balance their shifting defensive/offensive interests and accommodate each other, the Big Three have been increasingly adapting their conceptualizations of personal data and recalibrating their approaches to regulate cross-border data flows. When addressing Chinese digital and tech firms operating in its home market, the U.S. increasingly subscribes to a security-oriented conceptualization of data, and assertively deploys national security review mechanisms to scrutinize potential transfers of sensitive personal data to Chinese firms and/or the PRC government.[2295]

Likewise, the EU becomes increasingly vigilant to national security threats implicated by massive personal data held by foreign private actors, and switches to a security-oriented framing of data to address these challenges and risks. To that end, Europe has strengthened foreign investment screening mechanisms at both the EU and member state levels, guarding the access to sensitive personal data against Chinese investors.[2296] Meanwhile, both the EU and its key member states (such as German and France) increasingly emphasize the importance of "digital sovereignty", striving to nurture domestic digital platforms, decrease reliance on U.S. tech giants, and build a European cloud computing infrastructure subject to EU law.[2297]

To facilitate transatlantic data flows between their divergent internal data privacy regimes, the U.S. and the EU managed to find a compromise solution to transfer European personal data for American companies. Such institutional arrangements feature a voluntary "opt-in" mechanism for participating firms to self-certify their adherence to EU data protection standards, backed up by American and European authorities' oversight and enforcement.[2298] Caught between an economic and a rights-oriented conceptualization of personal data, this institutional framework deploys mixed institutions to implement European data protection norms. As such, this *sui generis* institution creates an exception for the protection of European personal data transferred to the U.S., enabling both sides to accommodate their institutional differences with respect to data privacy protection.

Finally, China increasingly embraces an economic framing of personal data, seeking to better leverage the commercial value underlying data flows. In international trade negotiations, it has acceded to U.S.-designed data transfer provisions to facilitate *inbound* data flows from Chinese

[2295] See *supra* chapter 1 ("A Battle of the Big Three"), section IV.A.
[2296] *Id.*, section IV.B.
[2297] *Id*.
[2298] See *supra* chapter 3 ("EU Forum-Shifting"), section IV.A.-B.

firms harvesting foreign data, despite its insistence on self-judging national security exceptions to bracket its domestic measures restricting *outbound* data flows.[2299]

Overall, each great power utilizes these sorts of recalibrations to manage their shifting interests and/or accommodate each other, while their dominant conceptualizations and regulatory approaches remain largely intact. Rather than suggesting a paradigm shift, these secondary conceptualizations and corresponding measures co-exist with the Big Three's primary conceptual framings and regulatory approaches, adding an extra layer of complexity and nuance to the transnational system governing cross-border data flows.

****

How a government conceptualizes personal data and frames the TPDF system is typically a complex, iterative, and value-balancing process, as multiple interests could interact in various ways.[2300] Yet, despite the multi-dimensional relationship among different interests involved, these three major conceptualizations largely dominate the Big Three's TPDF policymaking, respectively, and figure prominently in global data governance discourses.

To devise the substantive rules and institutional design for cross-border data flows, a sovereign actor has to choose one (or more) conceptualization(s) and regulatory approach(es) among an array of competing paradigms, in ways that would determine different default rules and exceptions. Depending on how a sovereign actor conceptualizes what personal data is and what the TPDF system should be, it will embrace distinct "optimal" balance struck among three primary interests/values of personal data (i.e., economics, privacy, and national security), and adopt a legal paradigm to pursue different policy priorities. In this way, competing conceptual framings of personal data provide divergent answers to the question of *who* should control *how* data flows in the global economy.

II. COMPETITIVE LAWMAKING STRATEGIES TO SHAPE THE GOVERNING RULES IN THE TRANSNATIONAL REGIME COMPLEX

Absent universal rules or multilateral institutions devoted to governing cross-border data transfers, the decision-making processes have been increasingly caught between an array of non-hierarchical, parallel, and partially overlapping international, regional, and domestic institutions that are racing to establish their regulatory authority. Rather than a single, decomposable international regime that intersects with other disciplines, the emerging system regulating transborder personal data flows

[2299] *Id.*, section IV.C.

[2300] For instance, despite the dominance of commercial interests, the economic framing of personal data also serves the U.S. government's national security interests, as free data flows facilitate U.S. national security authorities' signals intelligence and surveillance of data. For the EU, aside from pursuing normative value (which is paramount), a rights-oriented conceptualization of personal data also functions to safeguard national security interests against foreign intelligence surveillance, while achieving important economic goals (i.e., advancing EU market integration, and facilitating internal data flows). In the case of China, though its national security interests largely determine a security-oriented framing, the latter may also be deployed to localize data to benefit domestic digital industry, while undermining foreign digital giants' competitive advantage. See *supra* chapter 3 ("EU's Forum-Shifting"), section II.B., section III.B.(A), and section IV; *supra* chapter 5 ("China's Data Sovereignty"), section III.B.; *infra* section IV.C.

is best understood as *a transnational regime complex* featuring crisscrossing rules and complex obligations, given the increasing density of institutions, agreements, and instruments to govern this multi-faceted issue-area.

In this context, the U.S., the EU, and China have been deploying competitive lawmaking strategies of "regime-" and "forum-shifting" to shape the emerging rules on their preferred terms. Unable to sufficiently advance their preferred interests and achieve their prioritized agendas at the existing multilateral venues, the Big Three have been moving the rulemaking processes to different international, regional, or domestic institutions, including trade treaties, data privacy regulations, and security-oriented laws. By setting the terms for cross-border personal data flows, these great powers strive to shape the transnational rulemaking processes in ways that reflect their visions, serve their prioritized interests, and take advantage of their institutional capacities.

A. The U.S.

Largely driven by the U.S. "digital trade agenda", the USTR has been shifting the rulemaking processes to the international trade regime, using trade agreements to promote free data flows and discipline foreign governments' practices of "digital protectionism". Initially, the U.S. pursued "*horizontal regime-shifting*", bringing the issue of cross-border data flows under the ambit of a multilateral trade agreement (i.e., GATS 1994). However, the pre-Internet GATS was relatively outdated with respect to modern data-driven business models, and proved increasingly insufficient to address novel regulatory challenges brought by transnational data flows. And as subsequent WTO negotiations have come to a stalemate since the 2000s, the focus of U.S. trade lawmaking efforts shifted to vertical forums of bilateral and regional trade negotiations, where it can maximize its market clout and amplify its negotiating power to obtain a better deal.

By negotiating different U.S.-led PTAs over time, the U.S. kept pushing for higher protection for cross-border data flows, while reinforcing regulatory scrutiny over domestic data restrictive measures. By design, a country's internal regulatory measures restricting data export must be justified as "legitimate public policy exceptions" under a three-prong test of non-arbitrariness/discrimination, non-trade-restrictiveness, and necessity.[2301] Meanwhile, since the USMCA, the U.S. advanced the APEC CBPR system as an institutional solution to protect privacy for data in transit, which heavily relies on business self-regulation and establishes a permissive international privacy floor as sufficient. At the international level, the U.S. promotes the CBPR as a better alternative to the EU's GDPR, hoping to transform the former from a regional mechanism to a widely accepted international data privacy standard.

B. The EU

Different from the U.S., the EU has been repositioning the rulemaking over international data flows to a regional data protection regime that governs the processing of personal data in Europe and beyond. Specifically, such transnational lawmaking processes were launched by a powerful coalition of privacy-oriented institutional actors in Europe, including national DPAs, the WP29 (reconfigured as the EDPB under the GDPR), the DG Just, and the ECJ. Dissatisfied with the

[2301] TPP, art. 14.11; USMCA, art. 19.11.

institutional *status quo ante* for data privacy protection, these actors hoped to push for higher protection standards, remedy regulatory loopholes, and reinforce monitoring and enforcement. To that end, they have deployed the lawmaking strategy of forum-shifting to create, develop, and reform European data protection regulations on their preferred terms, while leveraging their asymmetrical power resources (such as delegated regulatory authority, network ties, regulatory capacity, agenda-setting power, judicial power) to impose their preferences on the Union level.[2302]

At the outset, national DPAs repositioned the TPDF rulemaking processes from a multilateral treaty (Convention 108) to the European Union's legislative process, using the Union's unilateral legislation to foster regulatory convergence among various EU member states. By this virtue, the EU came to implement a comprehensive data protection regime at the supranational level, which ensures high-standard protection of personal data as a precondition for permitting cross-border data flows to a recipient jurisdiction. Treating the EU Data Protection Directive as a floor, pro-privacy institutional advocates continued to leverage their power resources to push their agenda through the EU's lawmaking processes, further leveling up the regulatory standards of EU data protection law. From the Data Protection Directive 1995 to the GDPR 2016, the applicable data protection standards become higher and more robust, and the EU's regulatory scrutiny over outbound personal data transfers also becomes shaper and more expansive, in pursuit of greater protection of Europeans' fundamental rights.

Meanwhile, through pro-fundamental-rights judicial lawmaking (exemplified by *Schrems I* and *II*), the ECJ has effectively shifted the ultimate decision-making authority to determine a data recipient jurisdiction's "adequacy" from the Commission to the Court itself, which focuses more closely on European fundamental rights, and thus, imposes more stringent protective standards for data export against foreign intelligence surveillance. In effect, these precedents have constitutionalized the Commission's "adequacy" standard, empowering EU privacy activists and national DPAs to challenge EU-U.S. data transfer agreements before European judiciaries. Further, *Schrems I* and *II* have launched an iterative process where the ECJ can repeatedly use its judicial power to ratchet up data privacy standards for transnational data transfer mechanisms adopted by the Commission in future cases.

C. China

In the case of China, its newly-established data governance framework is largely driven by the twin objectives of safeguarding national security (against various data-enabled vulnerabilities) and achieving informatization and national development goals (by leveraging big data), rather than Western liberal values or constitutional rights. Within the transnational regime complex, China, driven by such political and economic motivations, has been moving the governance of transnational data transfers to a domestic regulatory framework, deploying a security-oriented set of laws, institutions, and processes (which are more amenable to the government's control) to set the standards for data flows. The regulatory requirements are characterized by the default rules to localize the storage and processing of data collected within its territory, subject to limited exceptions of outbound data transfers under relatively onerous conditions.

[2302] See *supra* chapter 3 (EU Forum-Shifting), sections II to IV.

With the increasing prominence of "data sovereignty" in national cyberspace rulemaking, China has enacted a proliferation of legislation and regulations to govern the collection, storage, transfer, use, and management of data, constructing a comprehensive legal architecture to regulate data security and cybersecurity. Unlike previous piecemeal regulations, this new regime imposes *territorial* data localization requirements on sensitive and important domestic data (including large amounts of personal data) across all sectors by default. Cross-border data transfers are permitted only through the relatively burdensome and inelastic mechanisms of security assessments, certification, or standard contractual agreements, characterized by strict regulatory control, high compliance costs, and legal uncertainties. Moreover, Chinese authorities proactively implement national security review processes to screen overseas business transactions that would subject massive domestic data to a foreign government's jurisdiction, expanding and sharpening regulatory scrutiny over the local effects of *extraterritorial* data processing activities.

III. DIFFUSION OF THE BIG THREE'S REGULATORY APPROACHES IN THIRD COUNTRIES: THREE EMERGING REGULATORY "SPHERES OF INFLUENCE"

In the global regulatory environment, the Big Three's primary governance approaches to cross-border data flows have been increasingly diffusing among other follower countries, which are to varying degrees inclined to embrace the core normative and institutional elements of these models. Focused on this salient phenomenon of "policy diffusion", the project explores the underlying mechanisms and factors driving third countries' increasing emulation and adoption of the U.S., European, and Chinese regulatory approaches, explaining the emergence of three regulatory "spheres of influence" worldwide.

A. The U.S.

Through vertical forum-shifting, the U.S. managed to conclude bilateral, plurilateral, and regional PTAs on its desired terms, making its trade partner countries sign up to its template of TPDF rules. In this process, it is crucial for the U.S. to condition market access and preferential trade liberalization on the acceptance of its preferred rules, thus coercing and incentivizing its trading partners to converge to its regulatory standards. As such, through negotiations of U.S.-led PTAs, the U.S. was able to export its data transfer provisions to its trade partner countries, causing them to internalize its own preferences in their trade policymaking.

Even without the presence of the U.S. as a trade negotiating partner, a growing number of PTAs have incorporated U.S.-designed data transfer provisions, exemplified by the TPP's and USMCA's digital trade rules promoting free data flows and disciplining data localization.[2303] During the WTO JSI negotiations on e-commerce, many U.S. trading partners have also emulated these provisions in their proposed text for a digital trade agreement.[2304]

As such, the diffusion of U.S.-promoted digital trade rules (without the U.S. even being at the negotiating table) is largely due to third countries' general perception of these rules as the most

[2303] See *supra* chapter 2 ("U.S.-Led Regime- and Forum-Shifting"), section V. See TPP, arts. 14.11, 14.13; USMCA, arts. 19.11, 19.12.
[2304] See *supra* chapter 2 ("U.S.-Led Regime- and Forum-Shifting"), section V.

"advanced" model to foster digital trade flows and develop the digital economy, reflecting the prevalence of the neo-liberal trade discourse in global digital policymaking—at least until the most recent years. Given that the U.S. is widely seen as a forerunner state with a highly developed digital industry, third countries often imitate its digital trade rules, treating them as the successful experience of a "role model" regulator.

Meanwhile, when a direct competitor (e.g., a neighboring country) has adopted U.S.-designed template, a state may be under peer pressure to follow suit, so as to maintain its competitive advantage for developing its digital market. Also, governments of developed markets sharing similar regulatory concerns (e.g., foreign restrictive measures undermine their domestic export-oriented digital firms' competitive advantage) can learn a regulatory innovation from the U.S. (a leading digital economy), believing that adoption of such rules helps to address their common policy challenges.

Importantly, by getting more and more third countries on board with its preferred approach, Washington's capability to deploy U.S.-designed PTAs to set the regulatory standards for the global digital economy is substantially enhanced, establishing and expanding its regulatory "sphere of influence" in the arena of transnational data governance. In this way, the U.S. not only has used its domestic "digital trade agenda" to shape global trade rulemaking, but also empowers the international trade regime to make a powerful claim to govern cross-border data flows.

B. The EU

Since the implementation of the EU Data Protection Directive in the mid-1990s, European norms of data privacy protection have become the *de facto* international standards for many third countries to follow, and this trend has accelerated with the enactment of the GDPR in 2016. In this process of norms diffusion, European data protection law has been playing a paramount role, enabling Brussels to set the data protection standards (including the criteria for outbound personal data flows) for much of the rest of the world.

To begin with, the Brussels effect has enabled the EU to *unilaterally* regulate the global marketplace through the market mechanism, exporting European data protection standards to multinational corporations and third countries with economic ties with Europe. Further, during its *bilateral* "adequacy" negotiations and talks with third countries, the European Commission has conditioned unrestricted data flows from Europe on the adoption of EU-style data protection laws, thereby pressuring and incentivizing foreign governments to emulate European standards in their domestic legislations and regulations.

Likewise, Brussels has also linked accession of new EU members to implementation of EU-like data protection laws, and provided various forms of assistance to facilitate applicants' domestic legal reforms. Moreover, the global diffusion of EU data protection norms is also due to their accessibility and normative appeal, making them an easily transplantable and highly attractive model for emulation.

In these ways, European data protection regulations have empowered the EU to utilize and magnify its economic power, negotiating leverage, and ideational influence, thereby transforming its data privacy norms into the international standards.

C. China

As a rising trend, an increasing number of developing countries have been adopting, or are considering, domestic laws modelled on Chinese cybersecurity regulations, including the latter's core normative elements of cyber and data sovereignty, online content control, and data localization. At the core, the spread of China's data regulatory approach is due to a set of "push-and-pull" factors (exclusive of coercion). Notably, the PRC government has been proactively advocating for its vision of cyber and data governance at regional and international venues and institutions, spreading the *normative* components of the Chinese approach in global governance discourses.

Moreover, along the Digital Silk Road, Chinese tech firms are increasingly supplying "made-in-China" digital infrastructures and technologies to emerging markets, providing the *material* components required to exercise a nation-state's cyber and data sovereignty. Further, since its core tenets and principles promise to address important security, economic, and strategic concerns shared by many developing countries, China's vision of cyber and data sovereignty creates strong normative appeal to these governments, incentivizing them to model their nascent domestic regulations on the PRC's norms, policies, and practices.

Through these mechanisms and factors at work, China is empowered to exert indirect, yet important, influence on like-minded developing countries amenable to its international influence, shaping their emerging data governance frameworks with its own vision. As a result, in parallel to countries following the U.S. and European approaches, there arises Beijing's regulatory "sphere of influence" in the global regulatory environment, increasingly challenging Western data governance models' global dominance.

****

In sum, for the Big Three, the increasing diffusion of their primary regulatory approaches is largely the result of these great powers' norm promotion efforts, whether through coercive means (such as issue-linkage) or international advocacy. Meanwhile, such norm diffusion processes are also due to the perceived attractiveness and ideational power of these regulatory approaches, pushing and pulling a third country to come on board with the Big Three's preferred norms. In the case of China, the Beijing Effect is also important: when supplying digital infrastructures and technologies to emerging markets, Chinese tech firms often facilitate the spread of the Chinese data governance approach abroad, to the extent that their commercial interests overlap with the PRC government's norm promotion agenda. In these ways, the Big Three are increasingly capable of shaping third countries' nascent data governance norms and institutions based on their own visions and preferences, thereby influencing the emerging international standards on TPDF in the transnational regulatory arena.

IV. IMPLICATIONS OF THE REGIME COMPLEXITY FOR TRANSNATIONAL DATA GOVERNANCE

The emergence of three different lawmaking processes and their respective regulatory "spheres of influence" abroad reflects and reinforces the nature of the transnational system governing cross-border data flows as a regime complex. Over time, the regulation of this issue-area is increasingly caught between different sets of institutions, rules, and discourses prioritizing distinct interests, ranging from economics to privacy to national security. On the international level, the U.S., the EU, and China's regulatory approaches are increasingly gaining traction by getting more countries on board, vying to dominate transnational digital rulemaking based on their respective visions and preferences.

Before ending this section, it bears noting three salient characteristics of the current transnational regime complex governing this issue-area, which may generate significant normative and policy implications for domestic and international data regulations.

A. The Western Blocks vs. The Eastern Block?

The Big Three's "spheres of influence" are not necessarily mutually exclusive, but rather may partially overlap with each other. For instance, Japan, South Korea, New Zealand, and Canada have concluded regional or bilateral PTAs that contain U.S.-designed digital trade rules favoring free data flows and restricting data localization.[2305] Meanwhile, after modeling their domestic data regulations on European norms and institutions, these countries are recognized by the EU as providing an "adequate" level of data protection, thereby enjoying unrestricted personal data flows from Europe.[2306] In particular, Japan's Personal Information Protection Act—though revamped to be GDPR-like in many important aspects—expressly recognizes outbound data transfers to a CBPR-certified recipient entity as satisfying this law's required equivalent standard of data protection (which is modeled on the EU's "adequacy" requirements).[2307]

Likewise, while some Latin American countries (such as Chile, Peru, Mexico) have launched legal reforms to closely align their domestic data protection laws with EU regulations,[2308] they have also adopted U.S.-promoted data transfer provisions in their PTAs.[2309] In particular, Chile—despite being a member of CPTPP and DEPA—has recognized the fundamental rights status of the rights to privacy and personal data protection in its PTA with the EU, while adopting an EU-style self-judging exception clause, precluding any domestic measures of data privacy protection that a treaty

---

[2305] See CPTPP, arts. 14.11, 14.13; South Korea-Singapore Digital Partnership Agreement, arts. 14.14, 14.15. Compare with TPP, arts. 14.11, 14.13.
[2306] GDPR, Third Countries, https://gdpr-info.eu/issues/third-countries/ (outbound transfers to Canada are limited to commercial organizations). See Paul Schwartz, *Global Data Privacy: The EU Way*, 94 NEW YORK UNIVERSITY LAW REVIEW 771, 807 (2019).
[2307] *Japan—Data Protection Overview*, October 2022, https://www.dataguidance.com/notes/japan-data-protection-overview.
[2308] Arturo J. Carrillo and Matias Jackson, *Following the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, 16 VIENNA J. INT'L CONST. L. 177, 181, 193-94 (2022).
[2309] See CPTPP, arts. 14.11, 14.13; DEPA, arts. 4.3, 4.4.

party considers appropriate from international trade and investor-state dispute settlement altogether.[2310]

As shown by these instances, it is possible for third countries to follow both the American and European regulatory approaches to cross-border data flows simultaneously, suggesting that these two governance models may not be inherently incompatible with each other. For the U.S. and the EU, their major regulatory differences are how personal data should be protected, and how cross-border data flows should be regulated. Given the widely recognized legitimacy of EU data protection standards in transnational data governance,[2311] invoking U.S.-promoted data transfer provisions to strike down a foreign country's EU-style data privacy law can be highly controversial and politically sensitive, potentially triggering international backlash against the claimant country's trade policymaking.

Further, provided that the U.S. obtains an "adequacy" decision from a third country following the EU's model of data regulation, it would be even less incentivized to bring such a claim before an international trade tribunal, thus mitigating and alleviating the tensions between the American and European approaches. In that regard, it bears noting that even if third countries choose to follow the EU's "adequacy" standard for outbound data flows, it is up to each government to determine whether a recipient jurisdiction achieves "adequate" protection of personal data, and they are not obliged to strictly follow the EU's adequacy decisions. Given the U.S.'s substantial market clout, a third country (especially an important trade partner of the U.S. such as Japan or South Korea) may recognize the U.S. as ensuring adequate protection for personal data, thus allowing free data flows to the American market.

Alternatively, the U.S. and a third country can imitate the U.S.-EU Safe Harbor and Privacy Shield agreements, and implement similar institutional arrangements to facilitate personal data flows, thereby satisfying a foreign government's "adequacy" standard on data protection. In this respect, a notable example is the U.S.-Switzerland Privacy Shield agreement. Modeled on the U.S.-EU Safe Harbor and Privacy Shield agreements, this institutional framework was designed to bridge both sides' institutional differences on data protection, thus permitting unrestricted outbound data transfers from Switzerland (that has adopted an EU-style data protection law) to the U.S.[2312]

[2310] EU-Chile Advanced Framework Agreement, December 2022, art. 19.5, https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/chile/eu-chile-agreement/text-agreement_en. Compare with European Commission, *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*, art. B, https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf. See *supra* chapter 4 ("Implications of EU Data Protection Law"), section I.A.(B).(b).

[2311] See Schwartz, *supra* (the EU Way), 771 (noting that the EU's GDPR "is now widely regarded as a privacy law not just for the EU, but for the world"); ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 36, 99 (2008); see also *supra* chapter 4 ("Implications of EU Data Protection Law"), section II.B.-C.

[2312] *Id.*, 812; see Federal Data Protection and Information Commissioner, *Swiss-US Privacy Shield: New Legal Framework for the Transfer of Data to the USA*, https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows/transfer-of-data-to-the-usa/swiss-us-privacy-shield--new-framework-for-the-transfer-of-data-.html. Although Switzerland data protection authorities declared the U.S.-Switzerland Privacy Shield agreement as "inadequate" pursuant to the ECJ's decision of *Schrems II* (that invalidated the U.S.-EU Privacy Shield), as the U.S. and the EU came to agree on a Privacy Shield 2.0 agreement, the U.S. and Switzerland may follow suit and conclude a similar framework to transfer personal data. See *Swiss-U.S. Privacy Shield No Longer Considered Adequate by Swiss DPA*, HUNTON ANDREWS KURTH (September 8, 2020),

Finally, as with Japan, a third country may recognize the APEC CBPR mechanism as achieving an adequate level of protection for cross-border data transfers. As such, it is possible to reconcile the institutional tensions and potential conflicts between the U.S. and European regulatory approaches to transnational data flows.

However, there may be significant tensions between third countries emulating the Chinese regulatory approach and the legal requirements imposed by the U.S. and European data governance models,[2313] particularly given that the latter two regulatory approaches explicitly oppose China's policies and practices of data localization.[2314] In other words, developing countries adopting the Chinese data governance approach may find it challenging to satisfy USMCA-style data transfer commitments or the GDPR's data protection standards.[2315] Over time, we may also see more fragmentations in the substantive rules and institutions between states within the U.S. and the EU's regulatory "spheres of influence" and countries following the Chinese approach.

B. Legal Fragmentations, Regulatory Barriers, and Transaction Costs

In the transnational regime complex, the applicable regulatory standards for cross-border personal data transfers may become increasingly fragmented, generating a growing number of regulatory barriers at the national level for international digital trade and e-commerce flows.

With European data protection norms increasingly gaining predominance as a highly influential international standard, a growing number of third countries have modelled their domestic data privacy laws on the EU's GDPR, including the "adequacy" requirements for cross-border personal data transfers. As suggested by a 2021 study, most national data privacy laws have followed the EU model, and there are at least 61 non-EU jurisdictions whose laws permit or require adequacy reviews of foreign jurisdictions before allowing outbound transfers of personal data.[2316] However, the criteria for determining whether a recipient country achieves an "adequate" level of data protection are far from consistent.[2317] As a result, the global regulatory environment witnesses increasing splintering of the "adequacy" condition, with different countries defining and applying this standard in different ways that reflect their visions and serve their agendas.[2318]

Meanwhile, as noted earlier, more and more developing countries are emulating China's data governance approach, and have enacted various data localization measures, which often come in

---

https://www.huntonprivacyblog.com/2020/09/08/swiss-u-s-privacy-shield-no-longer-considered-adequate-by-swiss-dpa/; *FAQs—EU-U.S. Data Privacy Framework Updates (1-4)*, PRIVACY SHIELD FRAMEWORK (January 11, 2023), https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

[2313] For example, Vietnam may find it difficult to obtain an "adequacy" decision from the EU, as its cybersecurity regulations provide permissive grounds for the government to obtain personal data collected by digital firms. And it may be quite challenging for Vietnam to reconcile its domestic data governance framework with its CPTPP commitments for free data flows and against data localization. See Erie and Streinz, *supra*, 37.

[2314] See European Commission, *Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection (in EU Trade and Investment Agreements)*, art. A(1), https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf; CPTPP, arts. 14.11, 14.13.

[2315] See Erie and Streinz, *supra*, 37.

[2316] Chander and Schwartz, *supra*, 19.

[2317] *Id.*, 17.

[2318] *Id.*

different shapes and vary in their specific formulations and requirements.[2319] While such measures may serve security, political, and strategic interests of those governments, they can also function as regulatory barriers hindering unrestricted cross-border data flows, fragmenting the global regulatory environment.

While the spread of the U.S. regulatory approach (featuring binding, enforceable commitments to free data flows, regulatory scrutiny over domestic data restrictive measures, and the APEC CBPR mechanism to protect privacy for data in transit) is supposed to remove countries' regulatory barriers and foster regulatory convergence, this may not necessarily work as planned, largely due to three reasons. To begin with, as noted earlier, a third country may adopt the U.S. and European approaches simultaneously, showing that these two governance models are not inherently conflictual, but rather can be accommodated by a follower country.

Further, while the U.S. strives to promote the CBPR as an international standard to provide a minimum level of protection for cross-border personal data flows, this mechanism thus far only receives a lukewarm response from the international community. Currently, there are merely nine economies that have participated in the CBPR, including the U.S., Mexico, Canada, Japan, South Korea, Singapore, Australia, the Philippines, and Chinese Taipei.[2320]

Although the U.S. acclaims the CBPR system as a better approach than the GDPR,[2321] it is unclear how many third countries may embrace the CBPR and reject the EU's regulatory approach, particularly given the potency of the Brussels effect and their fear of losing unrestricted data flows to the prosperous European market (by virtue of the EU's "adequacy" requirements). Rather, a third country may be incentivized to follow both regulatory approaches simultaneously, to the extent that it wants to secure its access to both American and European markets and/or is attracted by the normative appeal of these great powers' visions and policy prescriptions.

Moreover, given that data security increasingly implicates national security, countries such as China may assertively invoke the self-judging essential security interest exception to shield their domestic data localization measures from international trade adjudication altogether. [2322] Particularly, in light of the precedents set by the U.S. in the U.S.-China trade war (such as the expansion of "national security" to include the protection of critical domestic infrastructures or industries, and the U.S. stance that invocations of "national security" are entirely non-reviewable),[2323] China and its follower countries could become more emboldened to advance this

[2319] See *supra* chapter 6 ("Policy Diffusion of the Chinese Approach"), section II.
[2320] Billy Minshall, *Asia-Pacific Economic Cooperation CBPR Goes Global: What You Need to Know*, REDGRAVE 2022, https://www.redgravellp.com/asia-pacific-economic-cooperation-cbpr-goes-global-what-you-need-know; Graham Greenleaf (@grahamgreenleaf), Twitter (April 22, 2022, 8:58 AM), https://twitter.com/grahamgreenleaf/status/1517306911506706432 ("Global CBPRs is a worthless re-heating of APEC CBPRs, which after 10 years has only 3 active economies with certified companies: USA (36); Japan (3); Singapore (4). Certification is to 1980 standards. Canada, Korea, the Philippines & Taiwan just pretend involvement.").
[2321] Clare Sullivan, *EU GDPR or APEC CBPR?,* 35 COMPUTER LAW AND SECURITY REVIEW 380, 381 (2019).
[2322] See e.g., CPTPP, art. 29.2.
[2323] Anthea Roberts et al., *Toward A Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECO. L. 655, 672 (2019).

position when defending their domestic data governance policies and practices, thereby undercutting the potency of U.S.-designed data transfer provisions in trade agreements.[2324]

In the transnational regulatory landscape, the spread of the Big Three's approaches therefore may create a growing number of divergent national regulations with varied rules, prescriptions, and requirements, featuring substantial legal fragmentations and increasingly complex obligations. These domestic measures can constitute regulatory barriers to cross-border data flows, increase the compliance costs for digital firms handling personal data, and impose a greater burden on small and medium companies that are often less well-resourced to navigate the regulatory thicket. Specifically, to comply with European- and Chinese-style regulatory requirements, digital firms may have to resort to the more burdensome, costly, and inelastic mechanisms of cross-border data transfers, such as binding corporate rules, standard contractual clauses, security assessments, and certification (or their functional equivalents). Alternatively, they may need to establish and maintain local data centers or data storage facilities, incurring considerable expenses, compliance costs, and administrative burdens. In this sense, while allowing different powerful actors to pursue their prioritized interests (such as privacy or national security), the transnational regime complex can undermine development goals and technological innovation on a global scale.

C. Divergent Interests of the Big Three Mean Long-Persistent Regime Complexity

Despite the greater fragmentations in the global regulatory environment, the Big Three do not seem likely to bridge their divergence with respect to TPDF regulation in the short- and medium-term,[2325] given their differing interests and values. Though none of them might completely dominate global policymaking initiatives on this matter, the Big Three can achieve their prioritized interests and agendas underlying cross-border data flows in the transnational regime complex.

While it might be infeasible to unify global regulatory standards based on its vision, the increasing dominance of the U.S. regulatory approach in international digital trade rulemaking still could enable the U.S. to facilitate and promote unrestricted transnational data flows to its own market, where American digital giants that are capable of harvesting worldwide data are headquartered. This allows the U.S. to leverage such data to extract economic interests, stimulate technological innovation,[2326] and achieve national security and strategic interests,[2327] while avoiding major institutional reforms to its domestic framework of data privacy protection.

In the case of the EU, although some third countries are applying the "adequacy" standard differently, application of European data protection regulations can ensure that EU-originated personal data would be subject to a relatively high level of protection (against foreign private and

[2324] That being said, such an invocation of the exception clause will inevitably trigger lots of controversies and even economic sanctions imposed by another great power like the U.S.

[2325] This is the case, though the U.S. and the EU may be able to find a commonly accepted institution for transatlantic personal data transfers. In fact, the U.S.-EU data transfer mechanisms are more of a compromise made by two great powers to create an institutional interface between two different regulatory approaches, in order to facilitate transatlantic commerce flows. However, neither can compel the other to completely converge to its own model.

[2326] See *supra* chapter 2 ("U.S.-led Regime- and Forum-Shifting"), section IV.A. ("The U.S. Digital Trade Agenda").

[2327] The Snowden revelations expose U.S. intelligence agencies' long-standing practices of mass surveillance of foreign data for national security and strategic purposes. Generally, global free data flows and the accumulation of a lion share of such data in the U.S. facilitate U.S. authorities' surveillance and signals intelligence practices.

public actors). Internally, utilizing European regulations to foster regulatory convergence on data privacy protection among EU Member States could further European market integration, promoting free data flows within the EU's single market. And the global spread of EU data privacy norms as the *de facto* international standards empowers Brussels to become a global rule-maker, to level the playing field for European companies competing abroad, and to legitimize and validate its regulatory agenda internationally.

When regulating cross-border data flows, the Chinese data governance framework could safeguard Beijing's security, political, and strategic interests from being undermined, while leveraging data to grow domestic digital industry and achieve various development objectives. Internationally, the increasing diffusion of the Chinese approach in third countries enables China to boost the legitimacy of its norms, policies, and vision, consolidate its claims for data sovereignty, and strengthen Beijing's soft power and influence, thereby turning the PRC into a rule-maker in global cyberspace governance and a cyber superpower.

As such, each regulatory approach serves the economic, normative, national security, and strategic interests of the Big Three in a nuanced, intertwined, and complex way, in light of their policy priorities, concerns, and motivations, as well as their capabilities and constraints. Such divergent interests have been driving these powerful governments to adopt and promote different rules, institutions, and discourses, vying to shape the rulemaking processes based on their visions, preferences, and capacities. As a result, the transnational regime complexity may become more multi-layered, fragmented, and complex in the years to come, featuring increasing regulatory competition and contentious rulemaking aimed to dominate the governance of this cross-cutting issue-area. For this reason, it might be infeasible for states to reach a multilateral trade agreement or an international data privacy convention to effectively bridge different countries' regulatory divergence over cross-border personal data flows.

Rather than a short-lived phenomenon, the transnational regime complex governing cross-border data flows may persist for a long time and continue to evolve into a more sophisticated version, unless the underlying interests driving a great power to adopt a particular approach are changed. For scholars trying to understand the contentious and dynamic rulemaking processes over this issue-area, they may need to think about the ways in which the transnational regime complexity shapes, and is in turn shaped by, the strategies of different nation-states, sub-state, supranational, and non-state actors to push for their preferred rules and visions. When devising substantive rules and regulatory institutions, policymakers have to carefully consider their country's specific needs, balance competing interests at stake, and understand how power dynamics underlying the rulemaking processes may shape legal and regulatory outcomes.

Bibliography

I. Monographs:

BRAITHWAITE, JOHN & DRAHOS, PETER, GLOBAL BUSINESS REGULATION (2000)

BENNETT, COLIN J, REGULATING PRIVACY (1992)

BRAFORD, ANU, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020)

BYGRAVE, LEE ANDREW, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE (2014)

CRAIG, PAUL & BÚRCA, GRÁINNE DE, EU LAW: TEXTS, CASES, AND MATERIALS (2008)

DREZNER, DANIEL W, ALL POLITICS IS GLOBAL: EXPLAINING INTERNATIONAL REGULATORY REGIMES (2007)

FABBRINI, FEDERICO, FUNDAMENTAL RIGHTS IN EUROPE (2014)

FARRELL, HENRY & NEWMAN, ABRAHAM, OF PRIVACY AND POWERS: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY (2019)

FLAHERTY, DAVID H, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES (1989)

FOUCAULT, MICHAEL, THE ARCHEOLOGY OF KNOWLEDGE AND THE DISCOURSE OF LANGUAGE (1972)

GOLDSMITH, JACK & WU, TIM, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006)

GREENLEAF, GRAHAM, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES (2014)

GRUBER, LLOYD, RULING THE WORLD: POWER POLITICS AND THE RISE OF SUPRANATIONAL INSTITUTIONS (2000)

HARRIS, D J, O'BOYLE, M & WARBRICK, C, LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2009)

HOEKMAN, BERNARD M, THE GENERAL AGREEMENT ON TRADE IN SERVICES, IN THE NEW WORLD TRADING SYSTEM: READINGS (1994)

HONDIUS, FRITS W, EMERGING DATA PROTECTION IN EUROPE (1995)

INKSTER, NIGEL, CHINA'S CYBER POWER (2016)

JABLONSKI, MICHAEL & POWERS, SHAWN M, REAL CYBER WAR (2015)

KAUFFMAN, STUART A, AT HOME IN THE UNIVERSE, THE SEARCH FOR LAWS OF SELF-ORGANIZATION AND COMPLEXITY (1995)

KUNER, CHRISTOPHER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAWS (2011)

LEE, KAI-FU, AI, SUPERPOWERS: CHINA, SILICON VALLEY AND NEW WORLD ORDER (2018)

MALCOLM, JEREMY, MULTI-STAKEHOLDER GOVERNANCE AND THE INTERNET GOVERNANCE FORUM (2008)

NEWMAN, ABRAHAM L, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY (2008)

OVERBEEK, JOHANNES, FREE TRADE VERSUS PROTECTIONISM (1999)

ROBERTS, ANTHEA, IS INTERNATIONAL LAW INTERNATIONAL? (2017)

ROBERTS, ANTHEA & LAMP, NICOLAS, SIX FACES OF GLOBALIZATION: WHO WINS, WHO LOSES, AND WHY IT MATTERS (2021)

ROBERTS, MARGARET E, CENSORED: DISTRACTION AND DIVERSION INSIDE CHINA'S GREAT FIREWALL (2018)

SELL, SUSAN K, PRIVATE POWER, PUBLIC LAW (2003)

SOLOVE, DANIEL & SCHWARTZ, PAUL M, INFORMATION PRIVACY LAW (2015)

STAMPS, JAMES ET AL., U.S. INT'L TRADE COMMISSION, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES (2013)

STEINMO, SVEN H, AMERICAN EXCEPTIONALISM RECONSIDERED: CULTURE OR INSTITUTIONS? (1994)

SWEET, ALEX STONE, GOVERNING WITH JUDGES (2000)

TUMLIR, JAN, PROTECTIONISM (1985)

VOGEL, DAVID, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1995)

WALTZ, KENNETH, THEORY OF INTERNATIONAL POLITICS (1979)

WEBER, ROLF H & STAIGER, DOMINIC, TRANSATLANTIC DATA PROTECTION IN PRACTICE (2017)

ZUBOFF, SHOSHANA, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (PUBLIC AFFAIRS 2019)

II. Book Chapters:

Bollen, Yelter, Ville, Ferdi De & Orbie, Jan, *EU Trade Policy: Persistent Liberalisation, Contentious Protectionism*, 38 J. EUR. INTEGRATION 279, 282, 287 (2016)

Burri, Mira, *Creating Data Flow Rules through Preferential Trade Agreements*, forthcoming in DATA SOVEREIGNTY ALONG THE DIGITAL SILK ROAD (Chander, Anupam & Sun, Haochen eds., 2022), https://digitaltradelaw.ch/wp-content/uploads/2022/09/Burri_Creating-Data-Flows-Rules-through-Preferential-Trade-Agreements.pdf

Creemers, Rogier, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY (Broeders, Dennis & van den Berg, Bibi eds, 2020)

Edwards, Lilian, *Data Protection: Enter the General Data Protection Regulation*, in LAW, POLICY AND THE INTERNET (Edward, Lilian ed., 2018)

Gao, Henry, *Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China*, in ARTIFICIAL INTELLIGENCE AND INTERNATIONAL ECONOMIC LAW 298 (Peng, Shin-yi et al. eds, 2021)

Gao, Henry, *Data Regulation with Chinese Characteristics*, in BIG DATA AND GLOBAL TRADE LAW 245 (Burri, Mira ed., 2021)

Hoekman, Bernard, *The General Agreement on Trade in Services*, *in* READINGS OF THE NEW WORLD TRADING SYSTEM (OECD 1994)

Kilian, Wolfgang, *Germany*, in GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION (Rule, James B & Greenleaf, Graham eds., 2008)

Laskai, Lorand, *Nailing Jello to the Wall*, in CHINA STORY YEARBOOK 2016: CONTROL (Golley, Jane, Jaivin, Linda & Tomba, Luigi eds., 2017)

Lee-Makiyama, Hosuk, *Cross-Border Data Flows in the Post-Bali Agenda*, *in* BUILDING ON BALI: A WORK PROGRAMME FOR THE WTO (Evenett, Simon J. & Jara, Alejandro eds., 2013)

Mueller, Milton, *China and Global Internet Governance: A Tiger by the Tail*, in ACCESS CONTESTED: SECURITY, IDENTITY, AND RESISTANCE IN ASIAN CYBERSPACE (Deibert, Ronald et al., eds, 2011)

Polanco, Rodrigo, *Regulatory Convergence of Data Rules in Latin America*, in BIG DATA AND GLOBAL TRADE LAW (Burri, Mira ed., 2021)

Streinz, Thomas, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, in MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP (Kingsbury, Benedict et al. eds., 2019)

Tuthill, L Lee, *Cross-Border Data Flows: What Role for Trade Rules?*, *in* RESEARCH HANDBOOK ON TRADE IN SERVICES (Sauvé, Pierre & Roy, Martin eds., 2016)

Wunsch-Vincent, Sacha & Hold, Arno, *Towards Coherent Rules for Digital Trade: Building on Efforts in Multilateral Versus Preferential Trade Negotiations*, *in* TRADE GOVERNANCE IN THE DIGITAL AGE (Burri, Mira & Cottier, Thomas eds., 2012)

III. Journal Articles:

Abbott, Kenneth W, *The Transnational Regime Complex for Climate Change*, 30 ENV'T & PLAN. C: GOV'T & POL'Y 571 (2012)

Alden, Chris & Large, Daniel, *On Becoming a Norms Maker: Chinese Foreign Policy, Norms Evolution and the Challenges of Security in Africa*, 221 CHINA QUARTERLY 123 (2015)

Aaronson, Susan Ariel, *Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14 WORLD TRADE REV. 671 (2015)

Aaronson, Susan Ariel, *What Are We Talking about When We Talk about Digital Protectionism?*, 18(4) WORLD TRADE REV. 541 (2019)

Aaronson, Susan Ariel & Leblond, Patrick, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21 J. INT'L ECO. L. 245 (2018)

Alter, Karen J & Raustiala, Kal, *The Rise of International Regime Complexity*, 14 ANNUAL REV. L. & SOCIAL SCIENCES 329, 334 (2018)

Alter, Karen J & Meunier, Sophie, *The Politics of International Regime Complexity*, 7(1) PERSPECTIVES ON POLITICS 13 (2009)

Arato, Julian, Claussen, Kathleen & Heath, Ben, *The Perils of Pandemic Exceptionalism*, 114 AM J. INT'L L. 627 (2020)

Azmeh, Shamel & Foster, Christopher, *The International Trade Regime and the Quest for Free Digital Trade*, 22 INT'L STUDIES REV. 1 (2019)

Barnard-Wills, David et al., *Data Protection Authority Perspectives on the Impact of Data Protection Reform on Cooperation in the EU*, 32 COMPUTER LAW & SECURITY REVIEW 587 (2016)

Benvensti, Eyal, *Democracy Captured: The Mega-Regional Agreements and the Future of Global Public Law*, 23 CONSTELLATIONS 58 (2016)

Benvensti, Eyal & Downs, George W, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595 (2007)

Bergkamp, Lucas, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, 18 COMPUTER L. & SECURITY REV. 31 (2002)

Birch, Kean et al., *Data as Asset? The Measurement, Governance, and Valuation of Digital Personal Data by Big Tech*, BIG DATA & SOCIETY 1 (2021)

Black, Julia, *Regulatory Conversations*, 29 J. L. & SOC'Y 163 (2002)

Blume, Peter, *Controller and Processor: Is There a Risk of Confusion?*, 3 INT'L DATA PRIVACY L. 140 (2013)

Blume, Peter, *Transnational Data Flow: Is There a Solution in Sight?*, 8 INT'L J. L. & INFO. TECH. 65 (2000)

Bousquet, Antoine & Curtis, Simon, *Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations*, 24 CAMBRIDGE REV. INT'L AFF. 44 (2011)

Braford, Anu, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2015)

Braford, Anu & Posner, Eric, *Universal Exceptionalism in International Law*, 52 HARV. INT'L L. J. 1 (2011)

Bratman, Benjamin E, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENNESSEE L. R. 623 (2002)

Burri, Mira, *Interfacing Privacy and Trade*, 53 CASE W. RES. J. INT'L L. 35 (2021)

Burri, Mira, *The Regulation of Data Flows Through Trade Agreements,* 48 GEO. J. INT'L L. 408 (2017)

Burri, Mira & Schär, Rahel, *The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*, 6 J. INFO. PLCY. 479 (2016)

Bygrave, Lee Andrew, *The "Strasbourg Effect" on Data Protection in light of the "Brussels Effect": Logic, Mechanics and Prospects*, 40 COMPUTER LAW & SECURITY REVIEW 1 (2021)

Cai, Congyan, *Enforcing a New National Security? China's National Security Law and International Law*, 10 J. E. ASIA & INT'L L. 65 (2017)

Cai, Cuihong, *Global Cyber Governance: China's Contribution and Approach*, 4 CHINA QUARTERLY INT'L STRATEGIC STUDIES 55 (2018)

Chaisse, Julien, *Demystifying Public Security Exception and Limitations on Capital Movement*, 37 U. PENN. J. INT'L L. 583, 596 (2015)

Carrillo, Arturo J & Jackson, Matias, *Following the Leader? Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America*, 16 VIENNA J. INT'L CONST. L. 177 (2022)

Chander, Anupam, *Is Data Localization A Solution for Schrems II?*, 23 J. INT'L ECON. L. 771 (2020)

Chander, Anupam & Lê, Uyên P, *Data Nationalism*, 64 EMORY L. J. 677 (2015)

Chander, Anupam & Schwartz, Paul M, *Privacy and/or Trade*, 90 U. CHICAGO L. R. 49 (2023).

Chander, Anupam, Kaminski, Margot E & McGeveran, William, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021)

Chow, Daniel, *How the United States Uses the Trans-Pacific Partnership to Contain China in International Trade*, 17 CHIC. J. INT'L L. 370 (2016)

Claussen, Kathleen, *Forgotten Statutes: Trade Law's Domestic (Re)turn*, 113 AJIL Unbound 40 (2019)

Creemers, Rogier, *China's Emerging Data Protection Framework*, 8 J. CYBERSECURITY 1 (2022)

Cohen, Harlan Grant, *Nations and Markets*, 23 J. INT'L ECO. L. 793 (2019)

Coleman, Andrew & Maogoto, Jackson N, *"Westphalian" Meets "Eastphalian" Sovereignty: China in a Globalized World*, 3 ASIAN J. INT'L L. 237 (2013)

Coleman, Danielle, *Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws*, 24 MICH. J. RACE & L. 416 (2019)

Daskal, Jennifer, *Borders and Bits*, 71 VANDERBILT L. REV. 179 (2018)

Deibert, Ronald J & Crete-Nishihata, Masashi, *Global Governance and the Spread of Cyberspace Controls*, 18 GLOBAL GOVERNANCE 339 (2012)

deLisle, Jacques, *China's Approach to International Law: A Historical Perspective*, 94 AM. SOC'Y INT'L L. PROC. 267 (2000)

Dobbin, Frank, Simmons, Beth A, & Garrett, Geoffrey, *The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning*, 33 ANNUAL REVIEW OF SOCIOLOGY 449 (2007)

Dragu, Tiberia & Lupu, Yonatan, *Digital Authoritarianism and the Future of Human Rights*, 75 INT'L ORG. 991 (2021)

Drahos, Peter, *Securing the Future of Intellectual Property: Intellectual Property Owners and Their Nodally Coordinated Enforcement Pyramid*, 36 CASE W. RES. J. INT'L L. 53 (2004)

Drezner, Daniel W, *The Power and Peril of International Regime Complexity*, 7 PERSPECTIVES ON POLITICS 65 (2009)

Eichensehr, Kristen, *The Cyber-Law of Nations*, 103 GEO. L. J. 317 (2015)

Erie, Matthew S & Streinz, Thomas, *The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance*, 54 NYU J. INT'L L. POLITICS 1 (2021)

Henry Farrell, *Constructing the International Foundations of E-Commerce—The EU-U.S. Safe Harbor Arrangement,* 57 INT'L ORG. 277 (2003)

Farrell, Henry & Newman, Abraham, *Making Global Markets: Historical Institutionalism in International Political Economy*, 17 REV. INT'L POLITICAL ECONOMY 609 (2010)

Farrell, Henry & Newman, Abraham, *Weaponized Globalization: Huawei and the Emerging Battler over 5G Networks*, 14 GLOBAL ASIA 8 (2019)

Flonk, Daniëlle, *Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control*, 97 INT'L AFFAIRS 1925 (2021)

Fu, Hualin & Cullen, Richard, *National Security Law in China,* 34 COLUM. J. TRANSNAT'L L. 453 (1996)

Fuster, Gloria González & Gutwirth, Serge, *Opening up Personal Data Protection: A Conceptual Controversy*, 29 COMPUTER L. & SECURITY REV. 531 (2013)

Evans, A C, *European Data Protection Law*, 29 AM. J. COMP. L. 571 (1981)

Gao, Henry, *Digital or Trade?, The Contrasting Approaches of China and US to Digital Trade*, 21 J. INT'L ECON. L. 297 (2018)

Gao, Raymond Yang, *Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era*, 13(1) TSINGHUA CHINA L. RE. 165 (2020).

Gao, Xinchuchu, *An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model*, 57 INT'L SPECTATOR 15 (2022)

Goldsmith, Jack, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998)

Golley, Jane et al., *Geoeconomics and the Australian University Sector: A "Geoeducation" Analysis*, 16 SECURITY CHALLENGES 24 (2020)

Gordon, M J, *China's Path to Market Socialism*, 35 CHALLENGE 53 (1992)

Gravett, Willem, *Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa*, 20 AFR. HUM. RIGHTS L. J. 125 (2020)

Greenleaf, Graham, *Now 157 Countries: Twelve Data Privacy Laws in 2021/2022*, 176 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORTS 1 (2022)

Greenleaf, Graham, *Five Years of the APEC Privacy Framework: Failure or Promise?*, 25 COMPUTER LAW & SECURITY REV. 28 (2009)

Guo, Baogang, *Political Legitimacy and China's Transition*, 8 J. CHINESE POLITICAL SCIENCE 1 (2003)

Haas, Peter M, *Introduction: Epistemic Communities and International Policy Coordination*, 46 INT'L ORG. 1, 3 (1992)

Health, Benton, *National Security and Economic Globalization: Toward Collision or Reconciliation?*, 42 FORDHAM INT'L L. J. 1431 (2019)

Health, Benton, *The New National Security Challenge to the Economic Order*, 129 YALE J. INT'L L. 1020 (2020)

Helfer, Lawrence R, *Regime Shifting in the International Intellectual Property System*, 7(1) PERSPECTIVES ON POLITICS 39 (2009)

Helfer, Lawrence R, *Regime Shifting: The TRIPs Agreement and New Dynamics of International Intellectual Property Lawmaking,* 29 YALE J. INT'L L. 1 (2004)

Hoecke, Mark Van & Warrington, Mark, *Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative La*w, 47 INT'L & COMP. L.Q. 495 (1998)

Huang, Zhixiong & Mačák, Kubo, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271 (2017)

James, Scott & Lake, David, *The Second Face of Hegemony: Britain Repeal of the Corn Laws and American Walker Tariff of 1846*, 43 INT'L ORG. 1 (1989)

Jones, Meg Leta & Kaminski, Margot E, *An American's Guide to the GDPR*, 98 Denver L. R. 93 (2021)

Johnson, David R & Post, David, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996)

Käll, Jannice, *The Materiality of Data as Property*, 61 HARV. INT'L L. J. FRONTIERS 1 (2020)

Kaminski, Margot E, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV 1529 (2019)

Kaminski, Margot E & Malgieri, Gianclaudio, *Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIVACY L. 125 (2021)

Kang, Jerry, *Information Privacy in Cyberspace Transactions*, 50 STANFORD L. R. 1193 (1998)

Keohane, Robert O & Victor, David G, *The Regime Complex for Climate Change*, 9 PERSP. POL. 7 (2011)

Kim, Rakhyun E & Mackey, Brenda, *International Environmental Law as a Complex Adaptive System*, 14 INT'L ENVTL. AGMTS.: POL. L. & ECON. 5 (2014)

King, Gary, Pan, Jennifer & Roberts, Margaret, *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 AM. POL. SCI. REV. 1 (2013)

Kirby, Michael, *Legal Aspects of Transborder Data Flows*, 5 INT'L COMPUTER L. J. 233 (1991)

Kokott, Juliane & Sobotta, Christoph, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INTERNATIONAL DATA PRIVACY LAW 222 (2013)

Krasner, Stephen D, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66 (1988)

Kwet, Michael, *Digital Colonialism: US Empire and the New Imperialism in the Global South*, 60 RACE & CLASS 3 (2019)

Laurer, Moritz & Seidl, Timo, *Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation*, 13 POLICY & INTERNET 1 (2021)

Lee, Jyh-An, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57 (2018)

Liu, Lizhi, *The Rise of Data Politics: Digital China and the World*, 56 STUDIES IN COMPARATIVE INT'L DEVELOPMENT 45 (2021)

Luttwak, Edward, *From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce*, 20 NATIONAL INTEREST 17 (1990)

Manners, Ian, *Normative Power Europe: A Contradiction in Terms?*, 40 J. COMMON MARKET STUDIES 235 (2002)

Marchetti, Juan A & Mavroidis, Petros C, *The Genesis of the GATS (General Agreement on Trade in Services)*, 22 EUR. J. INT'L L. 689 (2011)

McKune, Sarah & Ahmed, Shazeda, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMMUNICATION 3835 (2018)

Mishra, Neha, *The Trade—(Cyber)Security Dilemma and its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567 (2020)

Mitchell, Andrew & Hepburn, Jarrod, *Don't Fence Me in: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH. 182 (2017)

Mitchell, Andrew & Mishra, Neha, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VANDERBILT J. TRANSNAT'L L. 1073 (2018)

Mitchell, Andrew & Mishra, Neha, *Regulating Cross-Border Data Flows in a Data-Driven World*, 22 J. INT'L ECON. L. 389 (2019)

Morin, Jean-Frédéric, *Multilateralizing TRIPS-Plus Agreements: Is the US Strategy a Failure?*, 12 J. WORLD INTELL. PROP. 175 (2009)

Morin, Jean-Frédéric, Pauwelyn, Joost & Hollway, James, *The Trade Regime as a Complex Adaptive System: Exploration and Exploitation of Environmental Norms in Trade Agreements*, 20 J. INT'L ECON. L. 365 (2017)

Morse, Julia C & Keohane, Robert O, *Contested Multilateralism*, 9 REV. INT'L ORGAN. 385 (2014)

Muller, Milton & Grindal, Karl, *Data Flows and the Digital Economy: Information as a Mobile Factor of Production*, 21 DIGITAL POLICY, REGULATION & GOVERNANCE 71 (2019)

Newman, Andrew, *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, INT'L ORGAN. 103 (2008)

Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010)

Pauwelyn, Joost, *At the Edge of Chaos? Foreign Investment Law as a Complex Adaptive System, How It Emerged and How It Can Be Reformed*, 29 ICSID REV. 372 (2014)

Peltz-Steele, Richard J, *The Pond Betwixt: Differences in the U.S.-EU Data Protection/Safe Harbor Negotiation*, 19. J. INTERNET L. 1 (2015)

Peng, Shin-yi & Liu, Han-wei, *The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?*, 51 J. WORLD TRADE 183 (2017).

Pernot-Leplay, Emmanuel, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PENN. ST. J. L. & INT'L AFF. 49 (2020)

Puig, Sergio, *International Regime Complexity and Economic Law Enforcement*, 17 J. INT'L ECON. L. 491 (2014)

Qi, Aimin, Shao, Guosong & Zheng, Wentong, *Assessing China's Cybersecurity Law*, 24 COMPUTER LAW & SECURITY REVIEW 1342 (2018)

Raustiala, Kal & Victor, David G, *The Regime Complex for Plant Genetic Resources,* 58 INT'L ORG. 277 (2004)

Reding, Viviane, *The Upcoming Data Protection Reform for the European Union*, 1 INTERNATIONAL DATA PRIVACY LAW 3 (2011)

Reding, Viviane, *The European Data Protection Framework for the Twenty-First Century*, 2 INTERNATIONAL DATA PRIVACY LAW 119 (2012)

Reidenberg, Joel R, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6. HARV. J. L. & TECH. 287 (1993)

Reidenberg, Joel R, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STANFORD L. REV. 1315 (1999)

Richards, John E, *Toward a Positive Theory of International Institutions: Regulating International Aviation Markets*, 53(1) INT'L ORGAN. 1 (1999)

Ritter, Jeffrey & Mayer, Anna, *Regulating Data as Property: A New Construction for Moving Forward*, 16 DUKE LAW & TECHNOLOGY REVIEW 220 (2018)

Roberts, Anthea, *Clash of Paradigms: Actors and Analogies Shaping the Investment Treaty System*, 107 AM. J. INT'L L. 45 (2013)

Roberts, Anthea et al., *Toward A Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECO. L. 655 (2020)

Roberts, Anthea & John, Taylor St., *Complex Designers and Emergent Design: Reforming the Investment Treaty System*, 116 AM. J. INT'L L. 96 (2022)

Ryngaert, Cedric & Taylor, Mistale, *Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation?*, 114 AJIL Unbound 5 (2020)

Salacuse, Jeswald W, *The Emerging Global Regime for Investment*, 51 HARV. INT'L L. J. 427 (2010)

Schafer, Hans-Bernand, *Rules versus Standards in Rich and Poor Countries: Precise Legal Norms as Substitutes for Human Capital in Low-Income Countries*, 14 SUP. CT. ECON. REV. 113 (2006).

Schwartz, Paul M, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995)

Schwartz, Paul M, *Global Data Privacy—The EU Way*, 94 NYU L. R. 771 (2019).

Schwartz, Paul M, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013)

Schwartz, Paul M, *The Data Privacy Law of Brexit: Theories of Preference Change*, 22 THEORETICAL INQUIRIES IN LAW 111 (2021)

Schwartz, Paul M & Solove, Daniel J., *Reconciling Personal Information in the United States and European Union*, 102 CALI. L. R. 877 (2014)

Schwartz, Paul M & Peifer, Karl-Nikolaus, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 115 (2017)

Segal, Adam, *Chinese Computer Games: Keeping Safe in Cyberspace*, 91 FOREIGN AFF. 14 (2012)

Selby, John, *Data Localization Laws: Trade Barriers or Legitimate Response to Cybersecurity Risks, Or Both?*, 25 INT'L J. L. INFO. TECH. 213 (2017)

Sell, Susan K, *TRIPS Was Never Enough: Vertical Forum Shifting, FTAs, ACTA, and TTP*, 18 J. INTELL. PROP. L. 447 (2011)

Sen, Nivedita, *Understanding the Role of the WTO in International Data Flows,* 21 J. INT'L ECON. L. 323 (2018)

Shaffer, Gregory, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000)

Shaffer, Gregory, *Trade Law in A Data-Driven Economy: The Need for Modesty and Resilience*, 20 WORLD TRADE REV. 259 (2021)

Shen, Yi, *Cyber Sovereignty and the Governance of Global Cyberspace*, 1 CHIN. POLIT. SCI. REV. 81 (2016)

Shi, Serena Y, *Dragon's House of Cards: Perils of investing in Variable Interest Entities Domiciled in the People's Republic of China and Listed in the United States*, 37 FORDHAM INT'L L. J. 1265 (2014)

Simmons, Beth A, Dobbin, Frank & Garrett, Geoffrey, *Introduction: The International Diffusion of Liberalism*, 60(4) INT'L ORG. 781 (2006)

Slawotsky, Joel, *The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualization*, 20 CHINESE J. INT'L L. 3 (2021)

Steinberg, Richard, *In the Shadow of Law or Power? Consensus-Based Bargaining and Outcomes in the GATT/WTO*, 56 INT'L ORGAN. 339 (2002)

Steinberg, Richard, *Judicial Lawmaking at the WTO: Discursive, Constitutional, and Political Constraints*, 98 AM. J. INT'L L. 247 (2004)

Streinz, Thomas, *Designing international Economic Data Law*, 115 ASIL PROCEEDINGS 73 (2021)

Sullivan, Clare, *EU GDPR or APEC CBPR?—A Comparative Analysis of the Approach of the EU and APEC to Cross Border Data Transfers and Protection of Personal Data in the IoT Era,* 35 COMPUTER LAW & SECURITY REV. 380 (2019)

Tai, Katharin & Zhu, Yuan Yi, *A Historical Explanation of Chinese Cybersovereignty*, 22 INT'L RELATIONS ASIA-PACIFIC 469 (2022)

Mercer, Shannon Togawa, *The Limitations of European Data Protection as a Model for Global Privacy Regulation*, 114 AJIL UNBOUND 20, 23-24 (2020)

Tsang, Cheng-Yun & Chen, Ping-Kuei, *Understanding Policy Diffusion Mechanism of Financial Regulatory Innovation*, 30 ASIA PACIFIC LAW REV. 21 (2022).

Victor, Jacob M, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L. J. 513 (2013)

Wang, Anqi, *Cyber Sovereignty and Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L. J. 395 (2020)

Wang, Heng, *Selective Reshaping: China's Paradigm Shifting in International Economic Governance*, 23 J. INT'L ECON. L. 583 (2020)

Warren, Samuel D. & Brandeis, Louis D., *The Right to Privacy*, 4 HARVARD L. R. 193 (1890)

Whitman, James Q., *The Two Western Cultures of Privacy: Dignity versus Liberty,* 113 YALE L. J. 1151 (2004)

Wu, Mark, *The "China, Inc." Challenge to Global Trade Governance*, 57 HARV. INT'L L. J. 261 (2016)

Wu, Tim, *The World Trade Law of Censorship and Internet Filtering*, 7 CHIC. J. INT'L L. 263 (2006)

Wunsch-Vincent, Sacha, *The Digital Trade Agenda of the U.S.: Parallel Tracks of Bilateral, Regional and Multilateral Liberalization,* 1 AUSSENWIRTSCHAFT 7 (2003)

Yakovleva, Svetlana, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 U. MIAMI L. REV. 416 (2020)

Yakovleva, Svetlana, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade "Deals"?*, 17 WORLD TRADE REV. 477 (2018)

Zang, Dongsheng, *Divided by Common Language: "Capture" Theories in GATT/WTO and the Communicative Impasse*, 32 HASTINGS INT'L & COMPARATIVE L. REV. 423 (2009)

Zeng, Jinghan, Stevens, Tim & Chen, Yaru, *China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty"*, 45 POLITICS & POLICY 432 (2017)

IV. Research Papers and Policy Reports:

Aaronson, Susan Ariel, *Data Is Different—Why the World Needs a New Approach to Governing Cross-Border Data Flows*, CIGI PAPERS NO. 197 (November 2018), https://www.cigionline.org/sites/default/files/documents/paper%20no.197_0.pdf

Aaronson, Susan Ariel, *The Digital Trade Imbalance and Its Implications for Internet Governance*, CIGI PAPERS No. 25 (February 2016), https://www.cigionline.org/sites/default/files/gcig_no25_web_0.pdf

Aaronson, Susan Ariel, *Data Is Dangerous: Comparing the Risks That the United States, Canada and Germany See in Data Troves*, CIGI PAPER NO. 241 (April 15, 2020), https://www.cigionline.org/publications/data-dangerous-comparing-risks-united-states-canada-and-germany-see-data-troves/

Biden Administration Plans for an Indo-Pacific Economic Framework, CONGRESSIONAL RESEARCH SERVICE (February 25, 2022), https://crsreports.congress.gov/product/pdf/IN/IN11814

Chander, Anupam & Lê, Uyên P, *Breaking the Web: Data Localization vs. The Global Internet*, UC DAVIS LEGAL STUDIES RESEARCH PAPER SERIES, RESEARCH PAPER NO. 378 (April 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858

Chander, Anupam & Sun, Haochen *Sovereignty 2.0*, GEORGETOWN LAW FACULTY PUBLICATIONS AND OTHER WORKS. 2404, UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPER NO. 2021/041 (2021), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3422&context=facpub

Cai, Keming, *Jurisdictional Report: People's Republic of China*, in REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA (Clarisse Girot ed., 2018), https://abli.asia/abli-publications/regulation-of-cross-border-transfers-of-personal-data-in-asia-softcover/#

Creemers, Rogier, *China's Cyber Governance Institutions*, LEIDEN ASIA CENTRE REPORT (January 2021), https://leidenasiacentre.nl/report-chinas-cyber-governance-institutions/

China and the World: Inside the Dynamics of a Changing Relationship, MCKINSEY GLOBAL INSTITUTE (July 2019), https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx

China's Evolving Data Governance Regime, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (July 26, 2022), https://www.uscc.gov/research/chinas-evolving-data-governance-regime

Cory, Nigel, *Writing the Rules: Redefining Norms of Global Digital Governance*, in CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER, NATIONAL BUREAU FOR ASIAN RESEARCH (March 2022), https://www2.itif.org/2022-NBRsr97-china-digital-ambitions.pdf?_ga=2.204751381.480101597.1652729267-2102500758.1652729267#page=79.

Cory, Nigel & Dascoli, Luke, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, ITIF (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Digital Trade and U.S. Trade Policy, CONGRESSIONAL RESEARCH SERVICE (December 9, 2021), at 43, https://sgp.fas.org/crs/misc/R44565.pdf

Erixon, Fedrik & Lee-Makiyama, Hosuk, *Digital Authoritarianism: Human Rights, Geopolitics and Commerce*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, OCCASIONAL PAPER NO. 5/2011 (2011), https://ecipe.org/wp-content/uploads/2014/12/digital-authoritarianism-human-rights-geopolitics-and-commerce.pdf

Ferracane, Martina Francesca & van der Marel, Erik, *Regulating Personal Data: Data Models and Digital Services Trade*, WORLD BANK GROUP, WORLD DEVELOPMENT REPORT 2021 POLICY RESEARCH WORKING PAPER 9596 (March 2021), https://openknowledge.worldbank.org/handle/10986/35308

Ferracane, Martina Francesca & van der Marel, Erik, *Do Data Policy Restrictions Inhibit Trade in Services?,* EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY, DIGITAL TRADE ESTIMATES WORKING PAPER NO. 2 (October, 2018), https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf

Ferracane, Martina Francesca & van der Marel, Erik, *The Cost of Data Protectionism*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (October 2018), https://ecipe.org/blog/the-cost-of-data-protectionism/.

Ferracane, Martina Francesca & Lee-Makiyama, Hosuk, *China's Technology Protectionism and Its Non-Negotiable Rationales*, EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (June 2017), https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf

Gao, Henry, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, HENRICH FOUNDATION (January 18, 2022), https://www.hinrichfoundation.com/research/article/digital/data-sovereignty-trade-agreements-digital-kingdoms/

González, Javier López et al., *A Preliminary Mapping of Data Localisation Measures*, OECD TRADE POLICY PAPER (June 2022), https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en

He, Alex, *The Digital Silk Road and China's Influence on Standard Setting*, CIGI PAPER NO. 264 (April 4, 2022), https://www.cigionline.org/publications/the-digital-silk-road-and-chinas-influence-on-standard-setting/

Hellström, Jerker, *Sovereignty*, in THE DECODING CHINA DICTIONARY (Oud, Malin & Drinhausen, Katja eds., 2021), https://decodingchina.eu/

Hong, Yanqing, *The Cross Border Data Flows (Data Exit) Security Assessment: An Important Part of Protecting China's Basic Strategic Resources*, RESEARCH ALLIANCE FOR DATA GOVERNANCE AND CYBER SECURITY (January 4, 2018), http://www.dgcs-research.net/a/Opinion/2018/0103/59.html.

Hong, Yanqing, *Designing Risk-Based Critical Information Infrastructure Protection in China*, RESEARCH ALLIANCE FOR DATA GOVERNANCE AND CYBER SECURITY (January 22, 2018), http://www.dgcs-research.net/a/Opinion/2018/0115/86.html

Irion, Kristina, Yakovlev, Svetlana & Bartl, Marija, *Trade and Privacy: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements*, UNIVERSITY OF AMSTERDAM INSTITUTE FOR INFORMATION LAW (July 2016), https://www.ivir.nl/publicaties/download/trade_and_privacy.pdf

Lee, Jyh-An, *Great Firewall*, CHINESE UNIVERSITY OF HONG KONG FACULTY OF LAW RESEARCH PAPERS 2018-10, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192725

Mattoo, Aaditya & Schuknecht, Ludger, *Trade Policies for Electronic Commerce*, WORLD BANK DEVELOPMENT RESEARCH GROUP POLICY RESEARCH WORKING PAPER NO. 2380 (June 2000), http://documents.worldbank.org/curated/en/164411468767105932/pdf/multi-page.pdf

Moynihan, Harriet, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, CHATHAM HOUSE RESEARCH PAPER (December 2019), https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf

Mullerat, Ramón, *EU-US Data Protection: Vindicating Rights to Privacy*, 4(14) EUROPEAN UNION MIAMI ANALYSIS Papers (June, 2017), http://aei.pitt.edu/8197/1/Mullerat_EUdataLawEUMA2007edi.pdf

Nagai, Oki, *Japan Teams with RCEP Allies to Push China on Data Free Flow*, NIKKEI ASIA (December 30, 2020), https://asia.nikkei.com/Economy/Trade/Japan-teams-with-RCEP-allies-to-push-China-on-data-free-flow

O'Hara, Kieron & Hall, Wendy, *There Are Now Four Competing Visions of the Internet. How Should They Be Governed*, WORLD ECONOMIC FORUM (March 12, 2019), https://www.weforum.org/agenda/2019/03/there-are-now-four-competing-visions-of-the-Internet/

Polyakova, Alina & Meserole, Chris, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS INSTITUTION (August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/

Segal, Adam, *Chinese Cyber Diplomacy in a New Era of Uncertainty*, AEGIS PAPER SERIES NO. 1703, HOOVER INSTITUTION (June 2, 2017), https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf

Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES (2016), https://www.europarl.europa.eu/RegData/etudes/STUD/2016/535006/EXPO_STU(2016)535006_EN.pdf

Wu, Mark, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, ICTSD (November 2017), http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf.

V. Chinese-Language Scholarship and Commentaries:

Ran, Congjing, *Global Landscape of Data Sovereignty Governance, and China's Response*, PEOPLE'S FORUM (March 2, 2022), http://www.rmlt.com.cn/2022/0302/641108.shtml. [冉从敬，《数据主权治理的全球态势与中国应对》，《人民论坛》2022 年 3 月]

Tian, Linan, *Countering Data Hegemony, and Strengthening the Capacity of Data Security Governance*, PRC MINISTRY OF COMMERCE (July 28, 2022), http://exportcontrol.mofcom.gov.cn/article/zjsj/202207/698.html [田力男，《反对数据霸权，提升数据安全治理能力》，原刊于《光明日报》，转载于中华人民共和国商务部网站，2022 年 7 月]

Wu, Xuan, *The Construction of Personal Information Cross-Border Transfers Rules under a Digital Sovereign Perspective*, 15 TSINGHUA LAW REVIEW 74, 83 (2021) [吴玄，《数据主权视野下个人信息跨境规则的建构》，《清华法学》2021 年第 15 期]

VI. Internet Sources:

Cheng, Ron, *China's Cyber Sovereignty and Cross-Border Digital Trade*, LAWFARE (March 31, 2017), https://www.lawfareblog.com/china-cyber-sovereignty-and-cross-border-digital-trade

China's Approach to Global Governance, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/china-global-governance/

Farrell, Henry & Newman, Abraham, *Schrems II Offers An Opportunity—If the US Wants to Take It*, LAWFARE (July 28, 2020), https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it

Google, *Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information*, GOOGLE PUBLIC POLICY BLOG (November 15, 2010), https://goo.gl/9CGxam

Gribakov, Andrei, *Cross-Border Privacy Rules in Asia: An Overview*, LAWFARE (January 3, 2019), https://www.lawfareblog.com/cross-border-privacy-rules-asia-overview.

Hillman, Jonathan E, *A "China Model?" Beijing's Promotion of Alternative Global Norms and Standards*, TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (March 13, 2020), https://perma.cc/QZL3-GJ8U.

Holleyman, Robert, *Lockout: How a New Wave of Trade Protectionism Is Spreading through the World's Fastest-Growing IT Markets*, BUSINESS SOFTWARE ALLIANCE TECHPOST (June 20, 2012), https://techpost.bsa.org/2012/06/20/lockout-market-access-report/.

Holleyman, Robert, *Remarks by Deputy U.S. Trade Representative Robert Holleyman to the New Democrat Network* ("Remarks"), USTR ARCHIVES, SPEECHES/TRANSCRIPTS (May 1, 2015), https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade

Hong, Yanqing, *Understanding the Political and Economic Considerations Behind the APEC Cross-Border Privacy Rules System*, WANGAN XUNLUREN (October 4, 2017), https://mp.weixin.qq.com/s/Gi59sRKAftyYcPhTVFmkTQ.

Information Office of the Chinese State Council, *White Paper on the Internet in China*, CHINA DAILY (June 8, 2010), https://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm

Kuner, Christopher, *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation*, EUROPEAN LAW BLOG (July 17, 2020), https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/

Kwet, Michael, *Digital Colonialism Is Threatening the Global South*, ALJAZEERA (March 13, 2019), https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south/.

Litt, David G & Monroe-Sheridan, A Reid, *The US-Japan Digital Trade Agreement and "Data Free Flow with Trust"*, USALI (February 3, 2022), https://usali.org/usali-perspectives-blog/the-us-japan-digital-trade-agreement-and-data-free-flow-with-trust.

Lu, Wei, *Cyber Sovereignty Must Rule Global Internet*, HUFFPOST (February 14, 2015), https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060

Luo, Yan & Yu, Zhijing, *China Issued the Draft Data Security Law*, COVINGTON UPDATES ON DEVELOPMENTS IN DATA PRIVACY AND CYBERSECURITY (July 3, 2020), http://www.insideprivacy.com/data-security/china-issued-the-draft- data-security-law/

Martinez-Herrera, Manuel, *From Habeas Data Action to Omnibus Data Protection: The Latin American Privacy (R)Evolution*, LEXOLOGY (October 5, 2011), https://www.lexology.com/library/detail.aspx?g=5f6d4229-5c79-4513-9b15-18dddd5c6a57.

Mueller, Milton, *A United Nations Committee for Internet- Related Policies? A Fair Assessment,* INTERNET GOVERNANCE PROJECT (October 29, 2011), https://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for- internet-related-policies-a-fair-assessment/

Park, Chaeri, *Knowledge Base: China's 'Global Data Security Initiative'* 全球数据安全倡议, DIGICHINA (March 31, 2022), https://digichina.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/.

Pfeifle, Sam, *Stefano Rodotà, Former Garante President and WP29 Chair, 1933—2017*, THE PRIVACY ADVISOR (July 19, 2017), https://iapp.org/news/a/stefano-rodota-former-garante-president-and-wp29-chair-1933-2017/

Roberts, Anthea et al., *Geoeconomics: The Chinese Strategy of Technological Advancement and Cybersecurity*, LAWFARE (December 3, 2018), https://www.lawfareblog.com/geoeconomics-chinese-strategy-technological-advancement-and-cybersecurity.

Sacks, Samm, *Beijing Wants to Rewrite the Rules of the Internet*, ATLANTIC (Jun 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

Sacks, Samm, Triolo, Paul & Webster, Graham, *Beyond the Worst-Case Assumptions on China's Cybersecurity Law*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (October 13, 2017), https://www.csis.org/blogs/technology-policy-blog/beyond-worst-case-assumptions-chinas-cybersecurity-law

Scott, Mark & Cerulus, Laurens, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (January 31, 2018), https://perma.cc/PKM3-BA3V.

Segal, Adam, *China's Alternative Cyber Governance Regime*, COUNCIL ON FOREIGN RELATIONS (March 13, 2020), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf

Streinz, Thomas, *RCEP's Contribution to Global Data Governance*, AFRONOMICSLAW (February 19, 2021), https://www.afronomicslaw.org/category/analysis/rceps-contribution-global-data-governance-0

Tiezzi, Shannon, *China's Bid to Write the Global Rules on Data Security*, DIPLOMAT (September 10, 2020), https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/

Triolo, Paul et al., *Xi Jinping Puts "Indigenous Innovation" and "Core Technologies" at the Center of Development Priorities*, NEW AMERICA (May 1, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/

Triolo, Paul & Webster, Graham, *Translation: China Proposes 'Global Data Security Initiative'*, DIGICHINA (September 7, 2020), https://digichina.stanford.edu/work/translation-china-proposes-global-data-security-initiative/

U.S. CHAMBER OF COMMERCE & HUNTON & WILLIAMS LLP, BUSINESS WITHOUT BORDERS: THE IMPORTANCE OF CROSS-BORDER DATA TRANSFERS TO GLOBAL PROSPERITY 2-3 (2014), https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf

U.S. Department of State, *The Clean Network*, https://2017-2021.state.gov/the-clean-network/index.html

United States Trade Representative, *Fact Sheet on the 2020 National Trade Estimate: Strong Binding Rules to Advance Digital Trade*, March 2020, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2020/march/fact-sheet-2020-national-trade-estimate-strong-binding-rules-advance-digital-trade

United States Trade Representative, *Fact Sheet on U.S.-Japan Digital Trade Agreement*, October 2019, https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2019/october/fact-sheet-us-japan-digital-trade-agreement

Wei, Yuxi, *Chinese Data Localization Law: Comprehensive but Ambiguous*, HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (February 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

Whether Global Initiative of Data Security Targets the U.S. "Clean Network" Program, the Response by Zhao, Lijian, CHINA ECONOMIC NET (September 9, 2020), http://www.ce.cn/xwzx/gnsz/gdxw/202009/09/t20200909_35706651.shtml

Yu, Zhijing, Liu, Vicky & Luo, Yan, *China Initiates Cybersecurity Review of Didi ChuXing and Three Other Chinese Mobile Applications*, COVINGTON: INSIDE PRIVACY (July 6, 2021), https://www.insideprivacy.com/international/china/china-initiates-cybersecurity-review-of-didi-chuxing-and-three-other-chinese-mobile-applications/