THE TRANSNATIONAL DATA GOVERNANCE PROBLEM

Douglas W. Arner,[†] *Giuliano G. Castellano*[††] *& Ēriks K. Selga*[†††]

ABSTRACT

The historical paradigm of data globalization is shattering. Fragmentation of transnational data flows and related governance frameworks is emerging globally as the result of fundamental differences in the governance mechanisms progressively deployed by the major economies and standard-setting jurisdictions to control the digital world. The irreconcilable positions of the United States, the European Union, and the People's Republic of China—further heightened by technological competition and geopolitical tension—are breaking down the global data economy and threaten to fracture its core infrastructure, the internet.

In this Article, we provide a systematic framework to analyze this emerging global landscape and assess its implications. Our analysis shows that each jurisdiction is characterized by an evolving and distinct data governance style based on its attitude towards markets and governance, the normative principles supporting the exercise of control over data, and the mode of regulating data. As these domestic governance styles consolidate into competing and conflicting data governance regimes, their transnational export and impact are fracturing the existing transnational data governance paradigm, which is based on free data movement, and hindering international coordination in the global data economy. We characterize this dynamic as the wicked problem of transnational data governance, which no single solution can address.

The Article highlights three approaches to address this wicked problem: (1) a bilateral approach that draws from the riparian system for water rights; (2) a plurilateral approach allowing the free circulation of data within sector-specific regulatory coalitions; (3) a multilateral approach, entailing either a hard law structure, with a "Digital Bretton Woods," or a soft law "Digital Stability Board." The implementation of a combination of these approaches offers a basis for a workable foundation for transnational data governance that harnesses the benefits of data globalization without undermining domestic sovereign priorities.

DOI: https://doi.org/10.15779/Z38GF0MX5G

† Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, Associate Director, HKU-Standard Chartered FinTech Academy, and Senior Fellow, Asia Global Institute, University of Hong Kong; Senior Visiting Fellow, University of Melbourne.

†† Associate Professor in Law, and Deputy Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

††† Research Fellow, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

Douglas W. Arner gratefully acknowledges the financial support of the Hong Kong Research Grants Council Senior Research Fellowship Scheme and the Qatar National Research Fund. Giuliano G. Castellano thanks the Hong Kong Research Grant Council for generous support through the General Research Fund (GRF n. 17607119).

TABLE OF CONTENTS

I. INTRODUCTION

Data permeates all aspects of modern economies and societies. As a result of decades of digitalization, data in digital form[1] are routinely created, gathered,

1. Data is the representation of information, concepts, and other phenomena in different (analog or digital) forms and mediums so that they are suitable for communication, interpretation, and processing by human beings or automated systems. *See generally* Chaim Zins, *Conceptual Approaches for Defining Data, Information, and Knowledge*, 58 J. AM. SOC'Y FOR INFO. SCI. & TECH. 479, 480 (2007) (exploring the foundations of information science and formulating

and shared across the globe to support core societal functions, including healthcare systems, transportation, international commerce, and national security. Digitalization brings together two interrelated processes: digitization, the transformation of analog information into digital form, and datafication, the application of quantitative and other analytics to data.[2] The "digitization of everything" [3] and the unprecedented expansion of datafication have led jurisdictions to acquire ever-expanding amounts of data, setting the stage for a new economy and the Fourth Industrial Revolution.[4] Thus, data is becoming a strategic asset that interlocks individuals, private actors, and public entities in global networks. Such a complex digital structure not only supports traditional economic activities but also gives rise to a new economic ecosystem (the data economy) where measurable information is sourced, analyzed, aggregated, and exchanged.[5]

---

definitions for data, information, and knowledge). In this paper, we refer to data in the digital format.

2. *See* VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA, 78 (2013) (defining digitization as "the process of converting analog information into zeros and ones of binary code so computers can handle it" and noting that "to datify a phenomenon is to put it in a quantified format to it can be tabulated and analyzed"). On the concept of datafication, *see also* Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POL'Y REV., 1 (2019) (defining datafication as the quantification of human life through digital information and, thus, noting that data increasingly interfaces with human behavior).

3. The "digitization of everything" generally refers to the wide and systematic transformation of any input—from music to biometric—into machine-readable electronic signal. This process is a step change, since it allows leverage on exponential computing power and, therefore, it is an agent of profound socio-economic changes. *See* KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION, 9 (2017) (noting that "technology and digitization will revolutionize everything.").

4. The development of infrastructure and technologies leveraging on and supporting data flows, together with digitization, are central dynamics characterizing the Fourth Industrial Revolution. *See* SCHWAB, *supra* note 3, at 12 (positing that the Fourth Industrial Revolution (2000-present) is characterized by mobile internet, sensors, actuators, machine learning, and artificial intelligence).

5. *See generally* Alexander Trauth-Goik, *Repudiating the Fourth Industrial Revolution Discourse: A New Episteme of Technological Progress*, WORLD FUTURES 55, 55-78 (2020) (presenting the growing interdependency of society and data, and suggesting a need for new ethical frameworks); SCHWAB, *supra* note 3; Albert Opher, Alex Chou, Andrew Onda & Krishna Sounderrajan, *The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization-A Perspective for Chief Digital Officers and Chief Technology Officers*, IBM (Mar. 13, 2016), https://hosteddocs.ittoolbox.com/rise_data_econ.pdf (discussing the emergence of a data economy based on the transformation of data into a strategic asset).

Societal dependence on data is an irreversible phenomenon, magnified by the diffusion of new technologies—such as the Internet of Things (IoT), distributed ledger technology (DLT), and artificial intelligence (AI)—and accelerated by the COVID-19 pandemic.[6] Data has therefore drawn comparisons to the most valuable resources in the world, including oil, oxygen, and water.[7] Like the counterparts of these analogies, national and international policymakers increasingly prioritize control over data, perhaps as *the* strategic priority, internationally and domestically. As framed by *The Economist* in 2017: "The world's most valuable resource is no longer oil, but data."[8] Put differently, data has become "the new oil."[9]

Over the past three decades, a techno-libertarian ethos has dominated transnational data governance, which is reflected in the free movement of data across the decentralized infrastructure of the internet. Absent an international legal framework governing data, domestic policymakers are developing different systems of rules and processes to extend their domestic and international jurisdictional control over the digital world. Policymakers are

6. LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 4 (2020) (outlining the growing dependence of society on data in day-to-day functions). On the role of technology in the context of the COVID-19 pandemic, see generally Douglas W. Arner, Ross P. Buckley, Andrew M. Dahdal & Dirk A. Zetzsche, *Digital Finance, COVID-19 and Existential Sustainability Crises: Setting the Agenda for the 2020s* (Univ. Hong Kong Fac. L. Rsch. Paper No. 2021/001), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783605 (examining how technology can help resolve the COVID-19 crisis at a micro and macro level); Douglas W. Arner, Janos Nathan Barberis, Julia Walker, Ross P. Buckley, Andrew M. Dahdal & Dirk A. Zetzsche, *Digital Finance & The COVID-19 Crisis* (Univ. Hong Kong Fac. L. Rsch. Paper 2020/017, Mar. 26, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3558889 (highlighting how the digitization of financial services may help address the challenges emerging from the COVID-19 crisis).

7. For data analogies, see generally Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373 (2013) (examining the development of data discussion following the emergence of new analogies); Jakob Svensson & Oriol Poveda Guillén, *What is Data and What Can It Be Used For? Key Questions in the Age of Burgeoning Data-Essentialism*, 2 J. DIGIT. SOC. RSCH. 65 (2020) (examining various data analogies and comparing them to actual data utility); Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows*, OECD TRADE POLICY PAPERS, No. 220 (2019) (examining the impact of data on trade and vice versa); R. J. ANDREWS, INFO WE TRUST: HOW TO INSPIRE THE WORLD WITH DATA 1–40 (2019) (comparing data to water, as it can be stored for later use).

8. *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (highlighting the rise in value of data).

9. *Data is Giving Rise to a New Economy*, THE ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy (presenting an argument for the growing importance of data and how it impacts data policy).

developing legal and regulatory frameworks to define rights and obligations for data holders and consumers;[10] competition policies have been triggered to curb data abuse by dominant incumbent firms;[11] and new rules to assert control over internal and external data flows and related infrastructure are being enacted.[12] Crucially, as these data governance frameworks develop and expand their reach across policy domains, they create new fault lines for geopolitical tensions and strategic competition centered around priorities like digital innovation, competitiveness, and cybersecurity. The urge for state actors to assert their sovereignty over data lies at the heart of these initiatives.[13] The result is the emergence of a global data governance framework that is transnational in nature and increasingly fragmented[14] by design.

---

10. Rights and obligations for data stakeholders extends across many policy domains. *See generally* Rene Abraham, Johannes Schneider & Jan vom Brocke, *Data governance: A conceptual framework, structured review, and research agenda*, 49 INT'L J. INFO. MGMT. 424, 424–38 (2019) (highlighting the evolving state of data governance across domains, within data science, and in organizational scopes); Larry Catá Backer, *And an Algorithm to Entangle them All? Social Credit, Data Driven Governance, and Legal Entanglement in Post-Law Legal Orders*, *in* ENTANGLED LEGALITIES: BEYOND THE STATE 79 (Nico Krish ed., 2022)/// (arguing that the emergence of data driven analytics and algorithmic techniques is reshaping the conception of data governance).

11. For instance, the FTC recently filed a complaint against Facebook in an ongoing federal antitrust case, alleging that Facebook resorted to illegal buy-or-develop schemes to maintain market dominance. *See* Press Release, Fed. Trade Comm'n, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate (Aug. 19, 2021), https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush.

12. *See infra* Section III.A for a discussion on digital sovereignty and the territorialization of internal and external data flows.

13. OECD, THE PATH TO BECOMING A DATA-DRIVEN PUBLIC SECTOR (2019); U.N. SECRETARY-GENERAL, DATA STRATEGY OF THE SECRETARY-GENERAL FOR ACTION BY EVERYONE, EVERYWHERE (May 2020) https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf (recognizing the rise of data as a strategic asset around the world and presenting a framework for jurisdictions to mobilize and secure data capabilities).

14. Originally birthed in public international law, fragmentation has been used to refer to the tendency for legal rules and regulatory provisions to develop across different sectorial axes in an uncoordinated fashion both within and across jurisdictions. *See generally* INT'L L. COMM'N, FRAGMENTATION OF INTERNATIONAL LAW: DIFFICULTIES ARISING FROM THE DIVERSIFICATION AND EXPANSION OF INTERNATIONAL LAW: REPORT STUDY GROUP ON THE FRAGMENTATION OF INTERNATIONAL LAW, at 10-28 U.N. Doc. A/CN.4/L.682 (2006) (providing an exhaustive analysis of the notion of "fragmentation of international law"); Eyal Benvenisti & George W. Downs, *The Empire's New Clothes: Political Economy and the Fragmentation of International Law*, 60 STAN. L. REV. 595 (2007); Martti Koskenniemi, *Fragmentation of International Law? Postmodern Anxieties*, 15 LEIDEN J. INT'L L. 553 (2002). In the context of

This Article advances a twofold argument to identify the challenge of transnational data governance. First, we posit that fragmentation stems from the emergence of distinct data governance styles in the three largest economies: the United States, the European Union, and China. The multiplication of domestic regulatory initiatives may appear to be the result of piecemeal reforms. However, drawing from the literature of "varieties of capitalism,"[15] regulatory governance, and modes of regulation,[16] we demonstrate that the approaches adopted in each jurisdiction reflect patterns of specific cultural, political, economic, and legal characteristics.[17]

---

sectoral fragmentation, see Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J., 999 (2021) (positing that the fragmentation of commercial law results in the emergence of systems of rules and principles that when come into contact give rise to a phenomenon termed "commercial law intersections"); Joshua Karton, *Sectoral Fragmentation in Transnational Contract Law*, 21 U. PA. J. BUS. L. 142 (2018) (describing how commercial law has split across sectorial lines both at domestic and international level).

15. The notion of "varieties of capitalism" was introduced by Peter Hall and David Soskice to analyze the institutional differences between "liberal market economies" and "coordinated market economies" in different socio-economic ambits. *See* PETER A. HALL & DAVID SOSKICE, VARIETIES OF CAPITALISM 8-20 (2001) (introducing two core types of capitalism—liberal and coordinated—and noting that liberal market economies are more apt to support radical innovation whereas coordinated market economies tend to support incremental innovation). The notion has been further developed and applied in different contexts. *See, e.g.,* Gregory Shaffer, *Governing the Interface of U.S.-China Trade Relations*, 115 AM. J. INT'L L. 622 (2021) (explaining the differences between capitalist models in the United States and China in the context of international trade relationships). *See also* BEYOND VARIETIES OF CAPITALISM: CONFLICT, CONTRADICTIONS, AND COMPLEMENTARITIES IN THE EUROPEAN ECONOMY (Bob Hancké, Martin Rhodes, and Mark Thatcher, eds., 2007) (offering an overview of the application of the varieties of capitalism and a critique in the European context).

16. Robert A. Kagan, *How Much Do National Styles of Law Matter?*, *in* REGULATORY ENCOUNTERS: MULTINATIONAL CORPORATIONS AND AMERICAN ADVERSARIAL LEGALISM, 1-30 (Robert A. Kagan & Lee Axelrad eds., 2002) (discussing implications of different national and regulatory systems); Julia Black, *Learning from Regulatory Disasters*, 10 POL'Y Q. 3 (2014) (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective); *see generally* Giuliano G. Castellano, Alain Jeunmaître & Bettina Lange, *Reforming European Union Financial Regulation: Thinking through Governance Models*, 23 EUR. BUS. L. REV. 409 (2012) (typifying the relationship between the institutional setting and the mode of regulation in the context of regulatory models in the EU).

17. For the notion of "regulatory styles," see generally Francesca Bignami & R. Daniel Kelemen, *Kagan's Atlantic Crossing: Adversarial Legalism, Eurolegalism, And Cooperative Legalism*, *in* VARIETIES OF LEGAL ORDER: THE POLITICS OF ADVERSARIAL AND BUREAUCRATIC LEGALISM (Jeb Barnes & Thomas F. Burke eds., 2017) (defining regulatory styles as making, crafting, and implementing laws and regulations, conducting litigation, adjudicating disputes, and using courts); Cary Coglianese & Robert A. Kagan, *Regulation and regulatory processes in* REGULATION AND REGULATORY PROCESSES (Cary Coglianese & Robert A. Kagan eds., 2007) (presenting an overview of characteristics of regulatory styles, including statutory design,

Historically, the United States has followed a laissez-faire approach to data and technology. This model, epitomized by Silicon Valley's technology champions—Google, Apple, Facebook/Meta, Amazon, Microsoft (GAFAM)—has nurtured the rise of the internet in its current paradigm: globalized, permissionless, and supportive of free trade.[18] Upon the blueprint offered by the Washington Consensus, the internet developed favoring minimal regulation over data and fostering a frictionless pro-business environment for transnational data flows.[19]

Owing to the evolving priorities and conflicting interests of major jurisdictions, the traditional transnational data governance paradigm is shattering. The increasing extension of sovereignty over data and networks by policymakers in China, the European Union, and the United States and the emergence of distinct governance styles at the domestic level result in a marked territorialization of data, thus irreversibly altering the laissez-faire status quo that has supported global data flow in the past two decades. The invasion of Ukraine in February 2022 has heightened existing geopolitical tensions fueling these conflictual dynamics.

In all three jurisdictions, data governance represents a central strategic priority. In the United States, the 2019 Federal Data Strategy encompasses a ten-year vision for leveraging data in policymaking, a paradigmatic shift towards data centralization in support of competitiveness and national security.[20] In the European Union, policy efforts have aimed at protecting both the rights of E.U. citizens and the free circulation of data within its "Single Market."[21] With the implementation of the General Data Protection

---

characteristics of regulated entities, and background political environment). We refer to data governance styles as the variables characterizing approaches to the policy and regulatory domain, involving private and public actors.

18. *See infra* Section II.B for a discussion on U.S. data governance styles.

19. Dani Rodrik, *Goodbye Washington Consensus, Hello Washington Confusion? A Review of the World Bank's Economic Growth in the 1990s: Learning from a Decade of Reform*, 44 J. ECON. LITERATURE 973 (2006) (arguing for a paradigmatic end to the dominating Washington Consensus, which was the international development mantra of "stabilizing, privatizing, and liberalizing" rules favoring the free-market models of the U.S.).

20. Amy O'Hara, *US Federal Data Policy: An Update on The Federal Data Strategy and The Evidence Act*, 5 INT'L J. POPULATION DATA SCI. 1, 1-15 (2020) (presenting how the Federal Data Strategy expresses a growing priority for federal agencies to collect and process data).

21. Brett Aho & Roberta Duffield, *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*, 49 ECON. & SOC'Y 187, 188-92 (2020) (outlining how the European

Regulation (GDPR) in 2016,[22] Brussels marked a major shift in its governance style. The GDPR, in fact, extends beyond the borders of the European Union, expanding its influence to the digital domain.[23] The European Union's 2020 Data Strategy aims to harmonize cross-border data flows and data sharing between its twenty-seven countries, both to protect core E.U. interests and support competitiveness, particularly vis-à-vis large technology companies—Big Tech—in the United States and China.[24] As extraterritoriality rules and adequacy standards apply to regulate the flow of data outside the Single Market, more jurisdictions are now adopting E.U. standards—a "Brussels effect."[25]

China's strategic approach aims at pursuing a broader developmental agenda. As large technology-intensive firms—such as Baidu, Alibaba, and Tencent (BATs)—have emerged as alternatives to GAFAM, technology has become a key component within the economic and social policies pursued by Beijing. The 2017 Cybersecurity Law[26] and the new Data Security Law and Personal Information Protection Law (PIPL),[27] both adopted in 2021, as

---

Union has adopted consumer and privacy-protection oriented regulation to counter growing data-surveillance architecture).

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) /1.

23. *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020) (arguing that the European Union is competing with other governance styles through opt-in rules to access its market).

24. Big Tech generally refers to the leading global tech companies. However, legislators are currently trying to define the boundaries of what makes Big Tech. *See generally* VALERIE C. BRANNON, CONG. RSCH, SERV., LSB10309, REGULATING BIG TECH: LEGAL IMPLICATIONS 1 (Sept. 11, 2019) (highlighting how legislators are using the amount of monthly users to define Big Tech, such as companies with "more than 30 million active monthly users in the U.S., more than 300 million active monthly users worldwide, or who have more than $500 million in global annual revenue"); Aho & Duffield, *supra* note 21 (outlining how the European Union has adopted consumer and privacy-protection oriented regulation to counter growing data-surveillance architecture).

25. *See infra* Section II.C for a discussion on the "Brussels effect."

26. Huárén míngònghéguó wǎngluò ānquán fǎ (华人民共和国网络安全法)(现行有效) [Cybersecurity Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) 2016 P.R.C. Laws (China), *translated in* Rogier Creemers, Graham Webster & Paul Triolo, DIGICHINA: STANFORD UNIVERSITY (June 28, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ [hereinafter PRC Cybersecurity Law].

27. Zhōnghuá rén míngònghéguó shùjù ānquán fǎ (中华人民共和国数据安全法)

highlighted by the release of a new State Council strategy[28] in August 2021, are central components of its 14th Five-Year Plan (2021–25),[29] in which technology is instrumental to both national security and socio-economic development, with a new focus on centralization and perhaps even autarky.[30] At the global level, a "Beijing effect" is taking shape in the form of a growing number of jurisdictions relying on technological and governance solutions developed in China.[31] As a result of this, Chinese digital influence has extended to the global market, challenging the U.S. incumbent position (under the Washington Consensus or the "California effect") and competing with the E.U. efforts to affirm domestic values in the global landscape.[32]

Second, we argue that emerging data governance regimes are on a collision course that is poised to compromise globalization and the global data

---

[Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong. June 10, 2021, effective Sept. 1, 2021) 2021 P.R.C. Laws (China), *translated in* DIGICHINA: STANFORD UNIVERSITY (June 29, 2021), https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ [hereinafter PRC Data Security Law]; Zhōnghuá rén míngònghéguó gèrén xìnxī bǎohù fǎ (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. of Nat'l People's Cong. Aug. 20, 2021, effective Nov. 1, 2021), 2021 P.R.C. Laws (China), *translated in* DIGICHINA: STANFORD UNIVERSITY (Aug. 20, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ [hereinafter PRC Personal Information Protection Law].

28. The Central Committee of the Communist Party of China and the State Council issued the "Implementation Outline for the Construction of a Government Ruled by Law (2021-2025)," XINHUA NEWS AGENCY (Aug. 11, 2021), xinhuanet.com/2021-08/11/c_1127752490.htm.

29. For the first time in the country's history, the new Five-Year Plan, released on March 13, 2021, does not set a specific GDP target. Instead, it establishes other goals, such as reducing unemployment, increasing life expectancy, lowering carbon-dioxide emissions, and bolstering technological innovation; *see* THE PEOPLE'S GOV'T FUJIAN PROVINCE, OUTLINE OF THE 14TH FIVE-YEAR PLAN (2021-2025) FOR NATIONAL ECONOMIC AND SOCIAL DEVELOPMENT AND VISION 2035 OF THE PEOPLE'S REPUBLIC OF CHINA (Aug. 9, 2021), https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.

30. *Id.*

31. The Beijing effect, similar to the Brussels effect, indicates the soft power exercised by China at the international level. It consists of a tendency of other countries to imitate and follow the initiatives developed in mainland China. *See generally* Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's' Digital Silk Road as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1, 1-17 (2021) (arguing that China is exporting its regulatory practice alongside infrastructure investments).

32. *Id.*

economy. The international digital landscape is already altering, given the expansionary influences—epitomized by the Brussels and Beijing effects—and ongoing efforts to decouple domestic infrastructures and technologies supporting data and their circulation. The result is a conflictual dynamic that tugs at the pillars of the shared decentralized, interconnected, and permissionless internet, with the potential to splinter the very foundation of the data-enabled global economy into areas divided by "digital Berlin walls."[33]

As idiosyncrasies solidify, the extraterritorial application of domestic rules reinforces the incompatibility of governance styles. For instance, the *Schrems* cases invalidated the E.U.-U.S. Privacy Shield framework deployed by American companies to comply with the GDPR.[34] In a similar vein, the extraterritorial effect of China's new 2021 Data Security Law in securing sensitive data reflects an even stronger approach to data localization and sovereignty.[35] These conflicts are canaries in the coal mine, anticipating much deeper fractures in the global data economy.

Although fragmentation is a ubiquitous phenomenon in international law, the emergence of competing and conflicting non-interoperable data governance regimes and their extraterritorial export result in a "wicked problem."[36] A clear-cut solution is unattainable, since domestic differences and

33. The idea of a "splinternet" foresees reversing the decentralization of internet architecture to allow domestic governments to control and divide traffic around the internet. *See generally* Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1397, 1422-27 (2021) (presenting how governments and companies are naturally striving towards controlling the internet); Stacie Hoffmann, Dominique Lazanski & Emily Taylor, *Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 J. CYBER POL'Y 239, 239-47 (2020) (arguing that the splinternet is also a result of diverging technical standards in internet infrastructure, which until now has been generally standardized globally); Kristalina Georgieva, Managing Director, IMF, From Fragmentation to Cooperation: Boosting Competition and Shared Prosperity (Dec. 6, 2021) https://www.imf.org/en/News/Articles/2021/12/06/sp120621-keynote-address-at-the-oecd-global-forum-on-competition (outlining the current trends of technological decoupling and creation of "digital Berlin walls," with negative impacts for the global GDP).

34. *See* Case C-363/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 73 (Oct. 6, 2015) (Schrems I); Case C-311/18 Data Prot. Comm'r v. Facebook Ireland Ltd., (July 16, 2020) (Schrems II); *see generally* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J. INT'L ECON. L. 771 (2020) (discussing the Schrems cases and discussing the consequent possibility of slowing data flows across the transatlantic).

35. *See infra* Section II for a deeper discussion of the Chinese Cybersecurity Law.

36. In general, wicked problems present specific characteristics, such as the lack of a clear understanding of the problem, the impossibility to determine a viable solution, or the inability to test progress against benchmarks. For a discussion of wicked problems in different policy domains, see Udo Pesch & Pieter E. Vermaas, *The Wickedness of Rittel and Webber's*

conflicting interests render a definitive solution very difficult. As governance styles develop and jurisdictions extend their sovereignty into the digital domain, previously permissionless international data flows become fractured. As data governance styles harden into conflicting, competing, non-interoperable transnational data governance regimes, national interests clash, and international coordination becomes even more difficult. Instead of aiming to work within a global internet-based data system, jurisdictions strive to change its parameters, with material consequences for the global data economy and globalization more broadly. This includes, for example, increasing transaction costs through additional compliance requirements within supply and value chains, or the total breakdown of data transmission that can disconnect commercial, financial, or other markets.[37]

There is no single solution to the wicked problem of transnational data governance. We identify three possible approaches that could be implemented discretely or in combination to address different critical aspects of the data governance problem. First, in approaching data as a natural resource, we submit that, from a governance standpoint, data presents issues similar to those posed by water (rather than oil), where the lack of an international framework leads to the proliferation of bilateral arrangements (on a case-by-case basis) to resolve jurisdictional conflicts. Building on the riparian practice of water rights management, coordination in transnational data governance could be improved through bilateral arrangements among the three largest

Dilemmas, 52 ADMIN. & SOC'Y 960, 960-72 (2020) (extending the nature of Rittel's wicked problem to institutional setups and broader social changes). In the context of data and technology, commentators have identified different wicked problems. *See* Jing Zhang & Yushim Kim, *Digital Government and Wicked Problems: Solution or Problem?*, 21 INFO. POLITY 215 (2016) (arguing that digital government has the potential to both empower and disenfranchise citizens); Konstantinos Komaitis, *The 'Wicked Problem' Of Data Localisation*, 2 J. CYBER POL'Y 355 (2017) (noting how localization policies may centralize power, rather than democratizing societies); Linnet Taylor, Time and Risk: Data Governance as a Super-Wicked Problem (Feb. 28, 2019) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344350, (indicating the potentially disruptive outcomes related to the exploitation of data).

37. The international financial system, for example, is utterly dependent on data flows—the decentralized participants of the SWIFT payment messaging system alone accounts for more than 25 billion payments a year. *See* Boaz B. Goldwater, *Incumbency or Innovation: Why a Collective Agency View of Cross-Border Payments Means Private Blockchains Cannot Prevail Notes*, 52 CORNELL INT'L L.J. 351, 352 (2019–2020) (arguing the unique nature of the international payments system and the role of SWIFT).

economies as well as among others inside or outside their respective data areas. Second, we suggest a regulatory coalition model built on regional or sectoral structures. This approach would build on a shared technological infrastructure, managed by an independent entity, where each jurisdiction decides which channels for data flows are opened and for which purpose. For instance, jurisdictions could maintain existing restrictions on the circulation of personal data, while allowing a free transnational flow of data for trade and financial purposes. Third, we consider a multilateral approach for transnational data governance. This solution could entail the establishment of a new "Digital Bretton Woods" (DBW).[38] In particular, a "hard law" framework,[39] consisting of treaty-based binding signatory states, would enhance international coordination, establish mechanisms to support data-related negotiations, and drive legal and regulatory harmonization of data governance. However, non-treaty-based "soft law" solutions are more realistic, given the difficulty to achieve an international consensus. In particular, under the aegis of the G20, a non-binding framework might be established.[40] In this context, a "Digital Stability Board" (DSB) would facilitate international coordination, while supporting the development of harmonized policies, principles, and standards related to data governance.[41] Looking forward, we envisage the most likely

38. The proposal of a Digital Bretton Woods has been animating current policy debate. *See* Rohinton P. Medhara & Taylor Owen, *A Post-COVID-19 Digital Bretton Woods*, CTR. FOR INT'L GOVERNANCE INNOVATION (Apr. 19, 2020), https://www.cigionline.org/articles/post-covid-19-digital-bretton-woods/ (noting that a new Digital Bretton Woods model could mitigate the negative implications of the digital revolution); Alex Pentland, Alex Lipton & Thomas Hardjono, *Time for a New, Digital Bretton Woods*, BARRON'S (June 18, 2021), https://www.barrons.com/articles/new-technologies-will-reshape-the-financial-ecosystem-and-the-world-with-it-51624023107; Brad Carr, *Digital Services & Data Connectivity: Facing into a Fragmented World*, LINKEDIN (MAR. 27, 2021), https://www.linkedin.com/pulse/digital-services-data-connectivity-facing-fragmented-world-brad-carr/ (highlighting the absence of a rulebook for the digital global economy and the growing negative consequences).

39. We follow Abbot's and Snidal's definition of "hard law" and "soft law" as non-binary choices along a continuum. Hard law denotes "legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority of interpreting and implementing the law." In turn, soft law is when "legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation." *See* Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421, 421-22 (2000).

40. *Id.*

41. Douglas W. Arner & Michael W. Taylor, *The Global Financial Crisis and the Financial Stability Board: Hardening the Soft Law of International Financial Regulation?*, 32 U. NEW S. WALES L.J., 488, 500-09 (2009) (arguing for the merits of a soft law multilateral regime as a partial substitute for hard law regimes).

result to be a combination of different approaches, extraterritorial, plurilateral, and multilateral, with the best (although not necessarily most likely) case being the creation of a coordinating DSB, along the lines of the G20–initiated Financial Stability Board.

This Article is composed of five parts. Section II outlines the evolving data governance styles and emerging regimes of the United States, China, and the European Union. Section III examines the competing and conflictual dynamics engendered by the emergence of increasingly competitive non-interoperable data governance regimes across the major economies. The analysis focuses on digital sovereignty as the driver for the emerging territorialization of data governance, the expanding role of national security concerns in shaping digital policies, and the splintered character of the global commons that is the internet. Section IV considers the wicked problem of transnational data governance, highlighting three possible approaches: (1) a bilateral approach that draws from the riparian system for water rights; (2) a plurilateral approach allowing the free circulation of data along sector-specific regulatory coalitions; (3) a multilateral approach, either based on a hard law structure, through a new DBW or soft law DSB. Section V concludes by suggesting that the most likely result is a combination of all three approaches. In the best case, coordination at the international level will lead to the establishment of a formal transnational framework; in the worst case, fractures will deepen and the global data economy will splinter into competing, non-interoperable blocs.

II. EVOLUTION OF TRANSNATIONAL DATA GOVERNANCE AND DATA GOVERNANCE STYLES

Over the past thirty years, globalization has been supported by a common approach to data. An extensive cyber regime complex consisting of international organizations, global corporations, non-governmental organizations, and governments alike has underpinned the current permissionless, open, and liberal internet.[42] The resulting free market for data has enabled

42. The concept of a cyber regime complex was originally introduced by Joseph Nye and has since been expanded. *See* Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, GLOB. COMM'N ON INTERNET GOVERNANCE, No. 1, 7 (May 20, 2014) (arguing for a need to shift analytical focus from a narrow internet governance regime to a broader cyber

data globalization across the global economy, led by large technology and data companies. The dominance of these companies in the new frontier of digital globalization has, not surprisingly, engendered reactions. Starting with the European Union and China, policymakers around the world and now even in the United States have acted to limit the power of such companies. As a result, data has become a focal point of domestic policies, resulting in the intensification of legislative interventions, regulatory initiatives, administrative enforcement actions, and court decisions.

Rather than sporadic attempts to regulate a new area or piecemeal reforms animated by political short-termism, these initiatives take distinct patterns, reflected in domestic data governance styles. Although jurisdictions share the common intent to assert domestic and international control over a strategic policy domain, the idiosyncratic nature of cultural, social, economic, and legal variables, combined with increasingly express strategic competition, generate different emphases on rights, obligations, and accountability mechanisms. Furthermore, the different roles and modi operandi of regulatory agencies, courts, and market-discipline mechanisms result in distinct approaches to attain stated policy objectives and interests.[43] Drawing from the notion of "regulatory styles,"[44] we identify emerging data governance styles as the result of several variables observed in each jurisdiction: (1) the general attitude towards markets and this evolving policy domain, as evidenced by the variety of capitalism and governance, policy priorities, and domestic antitrust and competitiveness policy; (2) principles guiding the public interventions in the data economy, as observed by the normative orientation defining the focus of

---

regime complex with a variety of issue-specific actors). *See infra* Section III.D for a more in-depth discussion.

43. This understanding is reflected in the regulatory governance literature. *See* Black, *supra* note 16. *See also* Karen Yeung, *'Hypernudge': Big Data as a Mode of Regulation by Design*, 20 INFO., COMMC'N & SOC'Y 118, 120 (2017) (noting that regulatory governance is a process based on three components: gathering information and monitoring; setting standards, goals, or targets; and changing behavior to meet targets).

44. On the notion of regulatory style, see Robert Kagan, *Introduction: Comparing National Styles of Regulation in Japan and the United States*, 22 L. & POL'Y 225, 226-40 (2000) (arguing that there is a difference in regulatory outcome based on the style of regulation in a jurisdiction); R. DANIEL KELEMEN, EUROLEGALISM: THE TRANSFORMATION OF LAW AND REGULATION IN THE EUROPEAN UNION (2011) (depicting differences, similarities and the convergence of US "adversarial legalism" and EU "eurolegalism"); Bignami & Kelemen, *supra* note 17 (defining regulatory styles as a pattern and a modus operandi affecting the design and implementation of laws, procedural approaches, adjudication of disputes, and the involvement of courts in the determination of regulatory outcomes).

protections established, and the control attributed to private actors over data; and (3) the regulatory approaches deployed to exercise control through a combination of rule design, and private and public enforcement strategies. Ultimately, a data governance style represents the synthesis of political structures, administrative frameworks, and regulatory approaches. Hence, these styles are not fixed; they evolve, as this Article's analysis of the United States, European Union, and China reveals. As styles evolve, they may harden into regimes, which we argue exists in data governance in the United States, European Union, and China.

By introducing the notion of data governance styles, this Section offers an analytical framework to understand the core dynamics affecting transnational data governance. The evolution of data governance styles in the United States, European Union, and China highlights their emerging differences, which are hardening into competing regimes that differ and conflict. The result is an ever-increasing fragmentation of the paradigm that supported data globalization thus far. This topic will be examined in Section III.

A. TRANSNATIONAL DATA GOVERNANCE AND DATA GOVERNANCE STYLES

Stemming from American approaches towards technology and data embodied on the internet and the foundations of the data economy and data globalization, a libertarian attitude has characterized the framework for transnational data governance since the 1990s, embracing a free market ideology.[45] This model follows a property-based approach in which all data is alienable. A dearth of government regulation of data movement created a model where data is treated the same as any other commodity and, as such, can be exchanged for value, provided markets are transparent and property rights are protected. This private sector-led approach, combined with the development of open access infrastructure in the form of the internet with limited public sector intrusion beyond funding and support for research and

45. The free market ideology of the internet stems from a "privatization" policy towards many aspects of the internet in the 1990's under the Clinton administration, whereby the U.S. reassigned maintenance of online naming and other infrastructural elements from the initial US defense contractors to the private and non-governmental sector, with minimal regulatory involvement. *See* SCOTT MALCOMSON, SPLINTERNET: HOW GEOPOLITICS AND COMMERCE ARE FRAGMENTING THE WORLD WIDE WEB 94–112 (2016).

development and a business-friendly environment, enabled the excesses of the 1990s dot-com bubble while also underpinning globalization.[46] From these foundations, global access to data has transformed the lives of billions, while enabling Big Tech to rise and dominate the global data commons.

Unlimited data access across jurisdictions through large platforms creates network effects. A consistent stream of new users produces new data, increasing the reliability and the utility of global platforms, thereby attracting more users. In this network-based economy, where data are transferred across jurisdictions and users, network operators acquire exclusive ownership and control over vast pools of data. Hence, the full alienability of data is central to this business model.

By leveraging the knowledge and marketability from data under their control, Big Tech continues to expand across sectors and borders alike. Issues of infrastructural control are also increasingly central to this process. GAFAM and BATs, for example, have built cloud hosting, content delivery, and interconnection platforms that are critical building blocks of the modern internet and digital economy. This architecture of consolidation and control has placed them into the role of content gatekeepers. Control over these elements is only growing, becoming especially critical to ensure the functioning of other IoT and internet reliant structures.

In response, for the past two decades, the European Union has sought to develop a regulatory toolset to curb the influence of private firms and governments over the data of its citizens. Before 2019, China largely followed the U.S. approach to domestic private data (combined with a very different approach to government use of data). Then, the approach shifted, with increasing government control over data flows circulating within China and crossing its borders. Eventually, as China sought to develop its national champions, GAFAM was not allowed within the domestic market. These differences have evolved into divergent and competing data governance styles.

In considering data governance styles, we highlight three sets of variables. The first set of variables pertains to the general attitude that public actors display towards markets and data flows. It describes the inherent cultural

46. *See* Richard Barbrook & Andy Cameron, *The Californian Ideology*, 6 SCI. AS CULTURE 44, 44-58 (1996) (arguing that the U.S. entrepreneurial class was promulgating a dotcom neoliberalist ideology that found the exploitation of information and knowledge as a utopian driver of growth and wealth).

anchor points characterizing the *why* of data governance in each jurisdiction. This dynamic is assessed through the prism of the political economy framework of "varieties of capitalism," where data governance measures are layered into strategic interactions of key institutional relationships. Each variety reflects the role of the state and market in the economy, as it emerges from institutional characteristics, political structures, and support to innovation.[47] The variety of capitalism is a blueprint upon which specific policy priorities are defined to support a public intervention in data governance, such as consumer protection, national security, or market development.[48] Finally, given the role of competition policies in curbing excessive dominance of data-intensive firms, the general attitude towards markets and data flow is reflected in antitrust law and competitiveness policies.[49]

The second variable refers to the main principles. These principles describe the core normative orientations between the actors, framing the *what* of general legal and non-legal standards of conduct. Principal alignment is characterized by the dialogic focus of a jurisdiction, which can be market, individual, or state-based. Each alignment propels the apportioning of rights and responsibilities that reinforce the primacy of their principles. The ultimate control over data, data agency, and data mobility, for example, differs across jurisdictions to reflect their core principles. As principles are put into regulatory action, they encapsulate an overarching toolbox of legal instruments that further define the regulatory taxonomy of a jurisdiction.

The third variable considers regulatory mechanisms. As emanations of their regulatory systems, regulatory mechanisms denote the proactive and reactive methods for *how* jurisdictions reach policy objectives and ensure adherence to principles. Regulatory mechanisms extend across a continuum between bottom-up, decentralized, and focused on private actors; or top-down, centered, and focused on the public sector. Within this continuum,

47. *See generally* Beáta Farkas, *Quality of Governance and Varieties of Capitalism in the European Union: Core and Periphery Division?*, 31 POST-COMMUNIST ECONS. 563 (2019) (describing varieties of capitalism and their developmental impact); HALL & SOSKICE, *supra* note 15.

48. BARBARA SCHULTE & MARINA SVENSSON, OF VISIONS AND VISIONARIES: INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) IN CHINA 1-9 (2021) (arguing that ICT realization reflects ideological policy preferences).

49. *See* FEDERICO ETRO, COMPETITION, INNOVATION, AND ANTITRUST: A THEORY OF MARKET LEADERS AND ITS POLICY IMPLICATIONS 6-26 (2007) (outlining that anti-trust and competition policy is intimately tied to market policy generally).

literature on regulation has identified a range of modes: command-and-control, whereby prescriptive formal measures narrowly describe rights and responsibilities; incentive-based (or market-based), characterized by the offer of financial or other benefits to secure certain behavior; and voluntary compliance, consisting of light regulatory frameworks and self-regulation.[47] A regulator's place on the continuum is triangulated by linking the design of rules and the approach to their implementation.[50]

The data governance styles of the United States, European Union, and China are converging in establishing data as a strategic priority. Each jurisdiction has set the normative foundations for data governance in higher-level areas including data interoperability, stewardship standards, and sharing.[51] These approaches are increasingly diverging in different policy areas.

B. UNITED STATES: EVOLVING LIBERAL MARKET CAPITALISM

The data governance style of the United States is characterized by liberal market capitalism. Disruption exercised by new business entrants is considered a benefit to innovation and economic growth and is thus fostered.[52] In line with this tradition, data flows are characterized by free market principles. The internet is, for example, considered a near-libertarian multistakeholder arena where public sector participation is limited to assuring a robust enabling infrastructure.[53]

---

50. On the connection of implemented rules and their design, see generally the literature tied to the design of regulatory discretion in public service; MICHAEL LIPSKY, STREET LEVEL BUREAUCRACY (1980) (arguing that public service workers in effect are policy decision makers, and thus the design of discretion provided to them is a regulatory choice); Sarah Giest & Nadine Raaphorst, *Unraveling the Hindering Factors of Digital Public Service Delivery at Street-Level: The Case of Electronic Health Records*, 1 POL'Y DESIGN & PRAC. 141 (2018) (arguing that accessibility of digital tools to public service workers is a further choice reflecting broader digital governance decisions); Peter J. May, *Mandate Design and Implementation: Enhancing Implementation Efforts and Shaping Regulatory Styles*, 12 J. OF POL'Y ANALYSIS & MGMT. 634 (1993) (arguing that "street-level" implementation of rules is an important aspect of regulatory assessment, as it may differ from codified rules).

51. OECD, *supra* note 13; U.N. Secretary-General, *supra* note 13; Casalini & González, *supra* note 7.

52. *See* Ingrid Schneider, *Democratic Governance of Digital Platforms and Artificial Intelligence?: Exploring Governance Models of China, the US, the EU and Mexico*, 12 EJ. OF EDEMOCRACY & OPEN GOV'T 6-14 (2020) (highlighting the authoritarian, libertarian, and hybrid models of platform governance).

53. *See* Eric Rosenbach & Shu Min Chong, *Governing Cyberspace: State Control vs. The Multistakeholder Model*, BELFER CTR. FOR SCI. & INT'L AFF. (Aug. 2019), https://

The prioritization of a free market is reflected in a dearth of government regulation over data movement. The U.S. data governance style manifests in a regulatory environment that has enabled the GAFAM firms to become Big Tech data market maker platforms that account for more than 55 percent of the used data capacity across the world.[54] The dynamic also underlies Zuboff's "surveillance capitalism," which argues that a dearth of regulatory oversight in data has resulted in a small concentration of corporate actors wielding substantial power over the social and economic behaviors of consumers around the world.[55]

The light-touch regulation has engendered a minimalist property-based regulatory principle as the anchor point for the United States.[56] The rights of the government, private, and natural persons are balanced at the locus of agency, which takes place at a contractual level. With narrow exceptions for public and national security, as long as a party is a titleholder to a certain asset, be it real estate, oil, or water—they can alienate this title. Personal or private data rights are thus no different from other property.[57] Hence, they are completely alienable if stipulated in a consensual agreement.

---

www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model (presenting different models of internet governance).

54. TELEGEOGRAPHY, THE STATE OF THE NETWORK 3 (2020), https://www2.telegeography.com/hubfs/assets/Ebooks/state-of-the-network-2020.pdf.

55. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 376-398 (1st ed. 2019) (arguing that the power of nation-states is increasingly dependent on their ability to wield data).

56. The approach has been confirmed by the treatment of data as property in State data privacy laws as well as the trade negotiating objectives of the Trade Promotion Authority legislation. *See* Illinois Biometric Information Privacy Act of 2008, 740 ILL. COMP. STAT. 14 (2008) (allowing a cause of action even where no actual injury occurred on the basis of protection of biometric information); California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100-1798.199 (West 2020) (granting individuals the right to request deletion of their personal information); P.L. 114-26, Title I (b)(6)(C) (setting the principal U.S. trade objective in digital trade by "refraining from implementing trade-related measures that impede trade . . . restrict cross-border data flows, or require local storage . . .").

57. There is ongoing discussion on the merits of data as a property right. *See* Andreas Boerding, Nicolai Culik, Christian Doepke, Thomas Hoeren & Tim Juelicher, *Data Ownership—A Property Rights Approach from a European Perspective*, 11 J. CIV. L. STUD. 323, 323-36 (2018) (drafting the dimensions of how law could establish data as a property right with positive access and negative restriction aspects). *See generally* P. Bernt Hugenholtz, *Against 'Data Property,' in* KRITIKA: ESSAYS ON INTELLECTUAL PROPERTY 48 (2018) (arguing against data as a property right as it would be restrictive on freedom of information and communication rights); Xiaolan Yu & Yun Zhao, *Dualism in Data Protection: Balancing the Right to Personal Data*

The predominance of the neoclassical laissez-faire approach put forward by the Chicago School of Economics over the past thirty years has shaped the U.S. data economy.[58] In particular, limited recourse to antitrust law in this field has been a contributing factor to the emergence of Big Tech. Both the Department of Justice and the Federal Trade Commission (FTC) enforce antitrust laws, with the latter also enforcing consumer protection rules. The Sherman Act and Clayton Act are relevant for antitrust enforcement but only saw serious use in the data market in 2019, when the FTC imposed a $5 billion fine against Facebook for failing to protect user privacy.[59] The FTC's settlement order also established an independent privacy committee of Facebook's board of directors, removing the CEO's unfettered control of privacy decisions.

The full alienability of data is supported by the adversarial legal system of the United States, as any limitation on contractual freedom is subject to judicial review. Enforcement in the U.S. is legalistic and judges are more likely to reverse administrative decisions curtailing individual rights.[60] Firms are comparable to political citizens and wield regulatory capacity through the adversarial court system.[61] Though firms generally comply with regulation, they are prepared to disobey in cases of principled disagreement, or where regulation seems arbitrary or unreasonable.[62] Lawsuits between tech firms testing the boundaries of law are also common with examples like the ongoing *Epic Games v. Apple* and *Epic Games v. Google* cases over preferential cross-platform treatment, or the historic *United States v. Microsoft Corp.* case over browser software bundling.[63]

---

and the Data Property Right, 35 COMPUT. L. & SEC. REV. (2019) (arguing that a data property protection system can be created under the Chinese Civil Code).

58. Sandra Marco Colino, *Towards a Global Big Tech Clampdown?*, AGENDA PÚBLICA (2021), https://agendapublica.elpais.com/noticia/16661/towards-global-big-tech-clampdown (highlighting a convergence of anti-trust concerns around the world regarding Big Tech data market power).

59. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

60. For this reason, interest groups often resort to court decisions to influence policy outcomes. *See* Coglianese & Kagan, *supra* note 17 (noting that the adversarial method is among the primary methods of negotiating regulatory change in the United States).

61. Coglianese & Kagan, *supra* note 17.

62. Coglianese & Kagan, *supra* note 17.

63. Friso Bostoen, *Epic v Apple: Antitrust's Latest Big Tech Battle Royale*, 5 EUR. COMP. & REG. L. REV. 79, 79-84 (2021) (describing the implications of the *Epic v. Apple* case for data

The genesis of the dominant philosophy underlying transnational governance of the flow of data, including personal data, stems from the United States, which has historically tacitly embraced the default regulatory doctrine of uninhibited flow of information across borders, with a general prohibition on data localization requirements.[64] Its negotiation of trade agreements has highlighted its approach to free data flows. The Trans-Pacific Partnership (TPP) as originally drafted and U.S.-Mexico-Canada Agreement (USMCA) regional trade agreements explicitly restrict prohibitions on cross-border transfer of information, forced localization requirements, and forced transfer of source codes.

Because of this adversarial system, proactive regulation is a tool of last resort in the United States, requiring both political will and careful consideration of market impacts. Regulation in the United States features the implementation of detailed provisions that, in an attempt to limit interpretation, increase the level of complexity through prescriptive,[65] rather than proscriptive, rules. Such prescriptive rules regarding data are rare; they are primarily observed in national security frameworks, such as the CLOUD Act, and the Foreign Intelligence Surveillance Act. Sectoral regulation is light, with examples like the California Consumer Privacy Act or the New York Department of Financial Services Cybersecurity Regulation scattered among states, and efforts at centralization have until recently been nascent.[66] Instead, data holders generally self-regulate.

---

companies); Salil K. Mehra, *Data Privacy and Antitrust in Comparative Perspective*, 53 CORNELL INT'L L.J. 133, 134-45 (2020) (outlining U.S. antitrust activity against Big Tech companies).

64. Marcelo Corrales Compagnucci, Timo Minssen, Claudia Seitz & Mateo Aboy, *Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield*, 4 EUR. PHARM. L. REV. 153, 154-59 (2020) (finding that SCCs will need to be consistently updated to incorporate necessary information security systems); Thomas Streinz, *The Evolution of European Data Law*, *in* EVOLUTION OF EU LAW 910-36 (Paul Craig & G. De Búrca eds., 3rd ed. 2021) (noting that E.U. data law gravitates around data protection).

65. Coglianese & Kagan, *supra* note 17.

66. *See* John Inglis, *Shining a Light on Cyber*, 14 STRATEGIC STUD. Q. 3, 3-11 (2020) (discussing how cyber-regulation is a growing priority in the United States, but remains underdeveloped as a strategic priority); Jared Bowman, *How the United States is Losing the Fight to Secure Cyberspace* 1-4 (2021) (arguing that the US data governance regime is light in comparison to other major economies); CYBERSPACE SOLARIUM COMMISSION, https://www.solarium.gov/ 1-19 (last visited Apr 25, 2021) (presenting the need and roadmap for data governance).

In the past decade, this core style has begun to evolve, largely as a reaction to the dominance of GAFAM and (more recently) competition with China. A few landmarks characterize the evolution of the U.S. data governance style and emerging regime. Under the Obama administration, the United States established two paradigmatic policy directions to extend this style. First, the administration escalated cybersecurity to a federal priority through the National Cyber Security Strategy, which has continued under the following administrations.[67] Second, the administration reinforced the free-trade focus on data by implementing a strict three-prong test for measures that restrict the free flow of information during the negotiation of the TPP.[68]

In 2019, the United States released the Federal Data Strategy. The strategy aims to shift the paradigm in how the government leverages data assets by prioritizing its collection and use and facilitating data for evidence-based policymaking.[69] The Federal Data Strategy is the culmination of several different legislative and administrative initiatives into a coherent foundational data governance document that moves away from a legacy system for the management of federal data by government agencies. It elaborates upon principles in three categories that aim to reflect and inform agency development and execution through all aspects of the data lifecycle, be they programmatic, statistical, or mission-support oriented. The strategy takes a soft approach, in line with a minimalist property-based paradigm of governing data systems, which balances rights together with commerce and state security interests. Where the European Union's GDPR, for example, requires that one of six legal bases be met for data processing regardless of other processes, under U.S. law, companies can process personal data by default.[70] The

67. Herb Lin, *How Biden's Cyber Strategy Echoes Trump's*, LAWFARE (Mar. 10, 2021), https://www.lawfareblog.com/how-bidens-cyber-strategy-echoes-trumps (discussing how the cyber strategies of the current and previous several terms are similar).

68. Erie & Streinz, *supra* note 31.

69. Russel T. Vought, *Federal Data Strategy - A Framework for Consistency*, OFF. OF MGMT. & BUDGET, https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-18.pdf. *See generally* O'Hara *supra* note 20 (describing the initial results of the Federal Data Strategy implementation, noting how a trajectory should be set towards creating a national secure data service).

70. Article 6 of GDPR lists the six legal bases as consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the

Supreme Court has previously struck state privacy law as being too restrictive of the freedom of speech, confirming its secondary nature.[71] The United States also lacks the dedicated institutional frameworks for data—privacy protection frameworks are piecemeal and sector-specific, while its enforcement is undertaken by the FTC and self-regulation.

The U.S. public sector's utilization of data is outlined in the Foundations of Evidence-Based Policymaking Act (or OPEN Government Data Act). The act requires that agencies develop evaluation plans linked to their strategic goals and that agencies create learning agendas focused on sequentially asking the "big questions," and then getting the information necessary to answer them.[72] The plan must define the data, methods, and analytical approaches used to acquire evidence and facilitate its use in policymaking. Depending on the goals of the agency, strategic evidence-based policymaking should enable them to better understand longer-term societal outcomes and the outputs of their programs. Under the Act, each agency must create an Open Data Plan in which data are cataloged for the public. Within them, data are categorized by tiers of sensitivity, which also decides who has the right to access it. As of yet, the applications for accessing statistical agency data are not centralized and differ between agencies.

Recently, the FTC sued Facebook for illegally maintaining a personal social networking monopoly through anticompetitive conduct.[73] The FTC is seeking a permanent injunction that would require divesting the assets of Instagram and WhatsApp—both of which are previous Facebook acquisitions.[74] Concurrently, the Department of Justice sued Google for maintaining monopolies through exclusionary practices in the search and advertising

free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

71. ZUBOFF, *supra* note 55, at 107.

72. The Act calls for inventorying and publishing all government information as open data. *See* OPEN Government Data Act, S. 2852 114th Cong. (2016). The provisions of the OPEN Government Data Act are now Title H of the Foundations for Evidence-Based Policymaking Act of 2018. H.R. 4174, 115th Cong (2019).

73. *See* Colino, *supra* note 58.

74. Press Release, Fed. Trade Comm'n, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization.

markets.[75] The new approach of the FTC and Justice Department highlights the beginnings of a paradigmatic shift in the U.S. approach to digital competition.

Thus, while the United States can be characterized as following a liberal free-market style, this is evolving, with increasing focuses on decreasing inequality and other tensions, competitiveness, security, and competition.

C. EUROPEAN UNION: COORDINATED MARKET CAPITALISM

The coordinated market capitalism of the European Union extends data governance to the dual priorities of free movement of data within its Single Market and protection of human rights. The removal of legal and technical barriers for the European Union under the four fundamental freedoms of movement for goods, capital, services, and people enables the existence of a Single Market in data. Under a concurrent aegis of human rights, data governance has also aimed to embed a rights-based approach to data reflecting core European cultural values and historical experiences as well as to harmonize and extend consumer protection and data privacy across the twenty-seven Member States.[76] This framework was a stepping stone for the development of an E.U.-wide data governance style in 1995 with the first Data Protection Directive.[77] It is this Directive that has been the most commonly adopted framework for data privacy and protection across the world over the subsequent twenty-five years.

At the same time, the European Union did not share the U.S.'s first-mover advantage in technology and data, and its private sector-oriented regulation has evolved to focus on shaping its market and requirements for companies aiming to trade in the European Union. Its "platform gap"—a shortage of market-dominant platforms and the influx of U.S. platforms—has triggered a regulatory response because changes in consumer preferences do not weaken

75. Press Release, Dept. of Just., Justice Department Sues Monopolist Google For Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

76. *See* Armin Von Bogdandy, *The European Union as a Human Rights Organization? Human Rights and the Core of the European Union*, 37 COMMON MKT. L. REV. 1307, 1309-16 (2000) (arguing that the EU is at its core focused on human rights).

77. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 431-40 (1994) (highlighting the role of the European Union in pioneering data protection).

the competitive advantage of dominant firms and abuse their power.[78] The platform gap also restricts the European Union in the development of new information-based technology that is data-heavy and depends on data to create positive feedback loops of better services and better data. Thus, the E.U. approach to data governance in the private sector aims to prevent data concentration and dominance, while also mandating and fragmenting data development for the benefit of new entrants, and concurrently reflects underlying E.U. social and cultural norms towards both the role of data and the role of the private sector. These norms have resulted in the development of an approach based on rights, use, and individual control as opposed to a property rights system, with this embedded in the series of E.U. data protection and privacy rules. Most recently, these norms have culminated in the GDPR for individual ownership and control of data, the Second Payment Services Directive for individual ownership and control of financial data, and the forthcoming data governance and data acts aiming to foster business-to-business and business-to-government data sharing.[79]

These dual priorities are enabled under a rights-based principle. As opposed to the property rights system of the United States, in the European Union, the use of data is constrained by statutory rights that limit the extent to which contractual agreement allows alienation of ownership and control. Though non-personal data are generally alienable, public authorities must retain access to certain data even if located in the other Member States and facilitate data portability procedures between service providers. Personal data, on the other hand, are inalienable from the individual they pertain to because they are considered a protected category. The European Union secures certain rights and control over data use regardless of a potential contractual agreement.[80]

---

78. A shortage of market dominant platforms and the influx of U.S. platforms has triggered a regulatory response because changes in consumer preferences do not weaken the competitive advantage of dominant firms and abuse their power. *See* José Van Dijck, *Seeing the Forest for the Trees: Visualizing Platformization and Its Governance*, NEW MEDIA & SOC'Y 2802, 2802-14 (2020) (highlighting the growing complex regimes established around platforms that are causing regulators to aim to reshape the platform system).

79. Streinz, *supra* note 64 (presenting an overview of the burgeoning E.U. data governance framework).

80. Interesting parallels can be drawn between the regime enacted by several E.U. jurisdictions regarding inalienable intellectual property licenses. *See* Andrea Tosato, *Secured*

In 2018, the European Union adopted regulations on the mobility of non-personal data.[81] In this framework, non-personal data can circulate freely within the Single Market; personal data, however, are subject to much stricter GDPR rules.[82] The GDPR allows the export of personal data only in compliance with the extraterritorial application of local data privacy rules. In particular, if personal data are processed overseas, the receiving jurisdiction must ensure that domestic rules meet adequacy requirements, whereby the transborder flow of personal data outside the Single Market can only occur if a certain level of protection is ensured.[83] When a jurisdiction meets such requirements and the European Commission grants the adequacy recognition, data can circulate freely between the Single Market and the third jurisdiction. The adequacy rules have been tested for their limits—Google resisted French requests to universally delist search results based on the E.U. right to be forgotten in *Google Inc. v. Commission nationale de l'informatique et des libertés* , limiting the result of adequacy decisions to within E.U. borders.[84] The GDPR also allows Member States to enact additional limits on the free circulation of personal data. Member States can, for example, enact data localization measures, in the context of health, financial services, or other sectors.[85]

The European Union's rights-based data approach was established by adopting a series of statutory instruments. GDPR structures consent-based data relationships between data subjects, controllers, and handlers, providing

Transactions and IP Licenses: Comparative Observations and Reform Suggestions, 81 L. & CONTEMP. PROBS. 155, 161-163 (2018).

81. Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303) 59.

82. Streinz, *supra* note 64.

83. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

84. In this case, the Court of Justice held that there is no obligation for Google to apply the European right to be forgotten globally, limiting the territorial withdrawal of information within the European Union. *See* Case C-507/17, Google v. CNIL, EU:C:2019:772 (Sept. 24, 2019).

85. Nigel Cory, Robert D. Atkinson and Daniel Castro, *Principles and Policies for "Data Free Flow With Trust,"* INFO. TECH. & INNOVATION FOUND. (May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust/ (highlighting the limits of data protection under the GDPR); Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/ (highlighting the transaction costs of data protection regimes).

subjects the right to be forgotten and personal data transfers at request.[86] The eIDAS regulation, for example, builds on this consent basis to establish an E.U.-wide digital ID regime for digital access to cross-border public and private services.[87] In turn, non-personal data are regulated under the Regulation framework for the free flow of non-personal data in the European Union, requiring frictionless movement of data across E.U. Member States. A series of forthcoming laws aim to further expand on the rules for domain-specific data spaces, public-private data sharing,[88] and the data duties of large gatekeeper platforms.[89]

The European Union also actively pursued competition cases as a reflection of its concerns over dominance and control of data and technology. Between 2017 and 2019, the European Commission fined Google three times for abusing its dominant position.[90] Germany's Federal Supreme Court upheld a 2019 decision against Facebook, confirming that the latter abused its dominant position in the German market, requiring Facebook to stop collecting data about its users without their consent.[91] The suite of rules,

86. *See* Max von Grafenstein, Alina Wenick & Christopher Olk, *Data Governance: Enhancing Innovation and Protecting Against Its Risks*, 54 INTERECONOMICS 228, 228-32 (2019) (presenting the need to reduce the risks of rampant data-based innovation).

87. These efforts aim to support the recently established E.U. 2030 digital targets, undertaking the digitization of key public services, e-health, and identity. *Europe's Digital Decade: Digital Targets for 2030*, EUR. COMM'N, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (last visited Mar. 26, 2021).

88. This occurs in the context of domain-specific initiatives, as it is the case of the Second Payments Services Directive. Broader, cross-sectoral initiatives include the Data Governance and upcoming Data Acts that, inter alia, aim to foster business-to-business and business-to-government data sharing on different areas. *See* Ginevra Bruzzone & Koenraad Debackere, *As Open as Possible, as Closed as Needed: Challenges of the EU Strategy for Data*, 56 LES NOUVELLES-J. LICENSING EXECS. SOC'Y 41, 41-48 (2021) (offering an analysis and outlining the weaknesses of current data sharing initiatives in the E.U.).

89. For instance, the upcoming Digital Markets and Services Acts aim to prevent anti-competitive behavior from large gatekeeper platforms, see *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data* COM (2020) 66 final (Feb. 19, 2020).

90. *See generally* Christophe Carugati, Competition Law and Economics of Big Data: A New Competition Rulebook (Nov. 16, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717420 (addressing competition law issues for Big Tech).

91. Klaus Wiedemann, *A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings* Bundeskartellamt v. Facebook *(Case KVR 69/19)*, 51 INT'L REV. INTELL. PROP. & COMPETITION L. 1168, 1174-80 (2020) (highlighting the ways

together with an active pursuit against anti-competitive practices places data companies aiming to compete under the E.U. framework into a share-by-design data market, where the growth of data concentration is significantly halted.

The E.U. approach to digital competition entails preventative measures under the precautionary principle.[92] A suite of regulations aims to create an environment that fosters the development of competitive data enterprise in the E.U. market while preventing the further concentration of GAFAM and Chinese competitors operating in Europe.[93] Beyond establishing the rights of individuals to control their personal data, the European Union set out several legislative initiatives to avert the singular aggregation of data-based market power.[94] These priorities also underpin the emerging E.U. aim to secure control over data produced in its territory under the concept of "digital sovereignty."[95] In 2020, the European Union announced a paradigmatic policy shift via novel strategies for data, by creating domain-specific "data spaces" that aggregate data within and across different sectors, with unique infrastructures, rules, data-sharing tools, platforms, and data interoperability for each.[96] Through such policies, the European Commission aims to close the "platform gap." The 2020 Platform to Business Regulation requires online platforms and search engines to provide clear and transparent terms and conditions regarding parameters for determining ranking and differentiated treatment.[97] The proposal for the Data Governance Act sets out the rules for

in which EU Member States can enact stronger data protection rules nationally than required by EU rules).

92. Aurelien Portuese, *Precautionary Antitrust: A Precautionary Tale in European Competition Policy*, *in* L. & ECON. REGUL. 203 (2021) (presenting the use of new regulatory and technological tools in the European Union antitrust regime as an example of a preference towards precaution over innovation and disruption).

93. Rocco Bellanova, Helena Carrapico & Denis Duez, *Digital/Sovereignty and European Security Integration: An Introduction*, 31 EUR. SEC. 337 (2022) (arguing that the inhibiting impacts of GAFAM on innovation and economic development have led to a more interventionist regulatory stance in the European Union).

94. *Id.*

95. Ursula von der Leyen, State of the Union Address by President von Der Leyen at the European Parliament Plenary (Sept. 16, 2020), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

96. *Id.*

97. *Platform-to-Business Trading Practices - Shaping Europe's Digital Future*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices (last visited June 23, 2021).

sharing data among businesses and foresees the creation of neutral data intermediaries that can act as trusts for this data.[98] Lastly, the Digital Markets Act establishes a criterion for qualifying large online platforms as "gatekeepers," which must permit third parties to interoperate within their ecosystems, allow business users to access data generated through the use of the platform, and prevent the treatment of self-services and products more favorably than those of third parties.[99]

At the core of the E.U. public-sector strategy is the cross-sectoral removal of legal and technical barriers to data sharing across organizations through the creation of domain-specific "data spaces" with unique infrastructures, rules, data-sharing tools, platforms, and data interoperability.[100] The European Commission posits these harmonized data-driven cloud-based ecosystems as the key to unlocking European "data pools," which enable benefits from big data analytics and machine learning. The approach to each data space will be unique, unified by principles of findability, accessibility, interoperability, and reusability.[101]

To operationalize the vision for its data governance strategy, the European Commission aims to create a single cross-sectoral governance framework for data access and use. Data will be made available for re-use for public and private sector participants through machine-readable formats and Application Programming Interfaces (APIs). The Commission will set additional horizontal and vertical data sharing requirements between public and private sectors through the forthcoming Data Act.[102] It will assess necessary measures

98. *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, COM (2020) 767 final (Nov. 25, 2020).

99. Luis Cabral, Justus Haucap, Geoffrey Parker, Georgios Petropoulos, Tommaso Valletti & Marshall Van Alstyne, *The EU Digital Markets Act: A Report from a Panel of Economic Experts*, EUR. COMM'N JOINT RSCH. CTR. (2021).

100. For a description of data spaces in the European Union, see generally *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, COM (2022) 68 final (Feb. 24, 2022), https://op.europa.eu/en/publication-detail/-/publication/d0f2ed7a-9664-11ec-b4e4-01aa75ed71a1/language-en (outlining the positive impacts of a data governance act on the European Union, finding that such regulation is necessary to ensure that more public and private actors benefit from Big Data and machine learning techniques).

101. *Id.*

102. *Id.*

for the establishment of specific data pools for machine learning and data analysis. Nine data spaces are initially planned, with more under consideration: industrial, Green Deal, mobility, health, financial, energy data, agriculture, public administration, and skills data.[103] These data spaces will feed into the recently established 2030 digital targets, which are aimed at the total digitization of key public services, e-health, and identity. The 2019 revision of the public sector information directive also requires that non-personal data held by public bodies be open for commercial and non-commercial reuse free of charge.[104]

These regulatory bundles mix outcome-based rules with enforced self-regulation for personal and non-personal data, respectively. The outcome-based regulation is enforced through institutional networks and entrusting E.U. courts to challenge and legitimize regulation.[105] The Court of Justice of the European Union (CJEU) and the European Court of Human Rights have, for example, repeatedly upheld fundamental privacy and consumer protection rights.[106] The European Commission has also fined Google for abuse of its dominant position in digital-advertising and comparison-shopping markets.[107] However, non-personal data are generally self-regulated in the European

103. *Id.*

104. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), 2019 O.J. (L 172) 56.

105. Chase Foster, Legalism Without Adversarialism: Public and Private Enforcement in the European Union 10-14 (June 2020) (working paper), https://www.chasefoster.com/_files/ugd/892c68_f9222e3d55d44d59ae020f39b64ebe4a.pdf (arguing that E.U. legislation does not encourage the private enforcement of public law, but courts still play an important role in legitimizing rules); Lincey Bastings, Ellen Mastenbroek & Esther Versluis, *The Other Face of Eurolegalism: The Multifaceted Convergence of National Enforcement Styles*, 11 REG. & GOVERNANCE 299, 304-11 (2017) (highlighting that there is a level of adversarialism present in the E.U. legal system).

106. Enumerated in Charter of Fundamental rights and European Convention on Human Rights. *See* OLIVER PATEL & NATHAN LEA, EU-U.S. PRIVACY SHIELD, BREXIT AND THE FUTURE OF TRANSATLANTIC DATA FLOWS 9 (2020) (highlighting human rights as a basis for the breakdown of the Privacy Shield regime).

107. For example, in 2019 the European Commission fined Google for abusing its data in online advertising. *See* Press Release, Eur. Comm'n, Antitrust: Google Fined €1.49 Billion for Online Advertising Abuse (Mar. 20, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

Union, with statutes creating a variety of "self-regulatory codes" for issues like data portability, or risk-based systems to prevent abuse of users.[108]

D. CHINA: FROM ORGANIZED TO CONTROLLED CAPITALISM?

China's evolving data governance style emerges from the primacy of the twin objectives of (1) stability (social, financial, economic, and national security) and (2) innovation, development, and competitiveness through a matrix of interlocking command-and-control regulations.[109] These goals manifest in a closely intertwined public and private sector relationship, where data in the domestic market before 2020 was largely treated similarly to data in the United States in the context of private markets, with full alienability and resulting in similar dynamics to those seen in the United States: the evolution of a small number of large dominant data firms.[110] At the same time, particularly over the past decade, the domestic market was largely protected from foreign competition (particularly from the United States). In parallel, from the standpoint of public sector data access and use, China is unique both in attitudes supporting such access and in the technical mechanisms and ability of the central government to access data for public policy interests. This nexus enables a vast digital autarky over what amounts to almost a third of global data flows.[111]

The Chinese data market is characterized by a combination of a property-based approach similar to that of the United States in the context of private-sector acquisition and control of data, combined with restriction of external competition in the form of import substitution and close cooperation with the state for broader governmental objectives. In China, the state works closely with the non-state sector. China blocks access to ten of the top twenty-five top global websites to support the evolution of a "parallel universe" of

108. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018 O.J. (L 303) 59.

109. *See* Rogier Creemers, *China's Conception of Cyber Sovereignty*, *in* DIGIT. TECHS. & GLOBAL POL. DIPL. 107, 107-15 (Dennis Broeders & Bibi van den Berg eds., 2020) (discussing the overarching goals of Chinese data governance policy).

110. *Id.*

111. Aho and Duffield, *supra* note 21; Wei Yin, *A comparison of the US and EU regulatory responses to China's state capitalism: implication, issue and direction*, 19 ASIA EUR. J. 1, 1–25 (2021) (discussing the size of China's state-centric form of capitalism).

domestically dominant Chinese platforms (e.g., Alibaba, Weibo, Baidu, and QQ).[112] The flexibility of skipping domestic development of desktop computing allowed China to leap toward innovation in mobile computing, enabling rapid adoption of new approaches.[113]

Both policy priorities are central to China's concept of "cyber sovereignty." Cyber sovereignty positions the digital environment and internet as areas for sovereigns to exercise their sovereign rights against other actors domestically and internationally. Through this lens, China enacts a high level of centralized control over data to protect national security interests, but also to guarantee its ability to intervene in the development of the domestic market.[114] Since 2017, China has taken an increasingly state-centered approach to cyber sovereignty, reflected in its development of a comprehensive regulatory governance framework. Three laws are the pillars of this approach: the 2017 Cybersecurity Law,[115] the 2021 Data Security Law, and the 2021 PIPL.[116] Based on these rules, China has also strived to limit private company dominance of data by bringing a series of regulatory actions against Ant, Tencent, Didi, and others.[117] The combination reflects an evolution in governance style that moves from a pro-private sector and innovation approach, albeit with state guidance, support, and involvement, to one much more expressly centered on the twin state objectives of stability and development.

Both priorities emanate from a state-centric normative orientation to the evolving framework, as reflected in a new state council policy framework in

112. Sebastian Hermes, Eric Clemons, Maximilian Schreieck, Simon Pfab, Maya Mitre, Markus Bohm, Manuel Wiesche & Helmu Krcmar, *Breeding Grounds of Digital Platforms: Exploring the Sources of American Platform Domination, China's Platform Self-Sufficiency, and Europe's Platform Gap*, EUR. CONF. ON INFO. SYS. JUNE 2020, https://aisel.aisnet.org/ecis2020_rp/132/ (discussing the access dynamic between online platforms around the world).

113. *Id.*

114. SCHULTE & SVENSSON, *supra* note 48.

115. PRC Cybersecurity Law, s*upra* note 26.

116. PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27.

117. China's tech crackdown saw record-large fines against the country's largest tech companies in fintech, ecommerce, ride hailing, social media, insurance, and other sectors. Many of these fines were related to the mishandling of consumer data, and anti-competitive practices. In the case of certain tech firms like Didi, the company was required to delist from the New York Stock Exchange and move to Hong Kong. For more, see *China's Big Tech Crackdown: A Complete Timeline*, THE CHINA PROJECT, https://thechinaproject.com/big-tech-crackdown-timeline/ (last visited Jan. 14, 2023).

August 2021.[118] While control over data under the emerging system follows the hybrid model of the European Union, attaching inalienable rights to personal data while allowing higher levels of alienability to non-personal data, ultimate control over data belongs to the central government. Not only does the government have access to data, but it also mandates data collection and analysis in both the public and private sectors. Though the government allows uninhibited flows internally, data can only leave or enter China with express government permission.[119]

China practices an increasingly restrictive stance on data mobility, as stipulated in the Data Security Law and the PIPL.[120] Any personal information generated within China must be stored within the physical jurisdictional territory, and any data export is under the centralized discretion of the Chinese data regulator, the Cyberspace Administration of China.[121] Concurrently, any processing of personal information outside of the Chinese jurisdiction requires that the processor retains representation in China.[122]

The state-centric principle is implemented through rule-based regulation. A sprawling framework of regulation under the umbrella priority of cyber-sovereignty sets data flows as a critical matter of national security, with corresponding duties for digital stakeholders. The Data Security Law establishes tiers of protected data, starting with "core state data" that includes issues of national security, national economy, or aspects of people's livelihoods that must undergo stringent cybersecurity approval procedures.[123] The

118. PRC Cybersecurity Law, s*upra* note 26; PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27; XINHUA NEWS AGENCY, *supra* note 28.

119. Angela Huyue Zhang, *Agility Over Stability: China's Great Reversal in Regulating the Platform Economy*, HARV. INT'L L.J. 26-40 (forthcoming 2022) (highlighting China's expanding regulatory oversight via antitrust, financial, and data regulation); Hermes et al., *supra* note 112.

120. For example, Article 25 of the Data Security Law stipulates the establishment of a "export controls" on data for national security interests. *See* PRC Data Security Law, *supra* note 27.

121. Article 38 of the PIPL stipulates that personal information can only be provided outside of China with approval or a security assessment by state institutions. *See* PRC Personal Information Protection Law, *supra* note 27.

122. *See* PRC Personal Information Protection Law, *supra* note 27 at art. 39.

123. PRC Data Security Law, *supra* note 27. See, in particular, rules related to national security, the lifeline of the national economy, important aspects of people's livelihoods under Chapters II, III, and IV.

Cybersecurity Law requires, for example, all "network operators"[124] that own, manage, or provide network services, to monitor and supervise the behavior of its users and "assist" in government requests.[125] While the PIPL establishes rules for personal data handling based on explicit consent, requiring short data retention time or allowing requests for deletion of personal data, it also provides for express circumventions if other laws, like the Cybersecurity Law, require such information.[126]

Rules are enforced under a command-and-control praxis. One manifestation of this mode is in statutes. Refusal to provide assistance to relevant departments makes network providers criminally liable under the Cybersecurity Law.[127] The Data Security Law, also expresses that the results of security reviews are "final." Another manifestation is through the "pervasive threat" of discretionary use of administrative tools by government agencies that can provide benefits or cause detriments to businesses, such as through rationing resources, licenses, or creating informal burdens.[128]

The Chinese regulatory approach to digital competitiveness manifests in "digital mercantilism" focused on securing economic stability.[129] The 2015 "Made in China 2025" strategy issued by the Chinese State Council expressly aims to support the integration of information technology and industry and promote breakthroughs in key information technology sectors.[130] Many of these strategies expressly depend on the mobilization of state-owned enterprises, the preferential allotment of capital to domestic companies, and the forced transfer agreement requiring foreign companies to transfer

124. Operators of critical information infrastructure are an additional separate category of subjects, dealing largely with state activities. *See* PRC Data Security Law, *supra* note 27 at art. 31.

125. *See* PRC Cybersecurity Law, s*upra* note 26.

126. *See* PRC Data Security Law, *supra* note 27; PRC Personal Information Protection Law, *supra* note 27.

127. *See* PRC Cybersecurity Law, s*upra* note 26.

128. *See* Xiaofan Zhao & Ye Qi, *Why Do Firms Obey?: The State of Regulatory Compliance Research in China*, 25 J. CHIN. POL. SCI. 339, 346-49 (2020) (highlighting informal methods of ensuring compliance in China).

129. *See* C.Y. Cyrus Chu & Po-Ching Lee, *E-Commerce Mercantilism-Practices and Causes*, J. INT'L TRADE L. & POL'Y 51, 53-59 (2020) (outlining a practice of digital mercantilism through asymmetrical internet access in China).

130. 2025 zhōngguózhìzào èr líng èr wǔ (中国制造) *Made in China 2025*, promulgated by the State Council on July 7, 2015, https://perma.cc/9PA3-WYBA, *translated in* CTR. FOR SEC. & EMERGING TECH. (Mar. 8, 2022), https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf.

intellectual property through forced joint ventures with local competitors.[131] Though China has committed to regulating against the forced transfer of technology by foreign firms, via the U.S.-China Trade Agreement of January 15, 2020, and the E.U.-China Comprehensive Agreement on Investment, forced IP handovers have not yet been addressed by regulatory measures in China. This has consequently resulted in a WTO dispute initiated by the United States.[132]

The quasi-public sector character of major tech platforms in China also adds an additional layer of complexity to regulating digital competition. Recently, the People's Bank of China, the country's central bank, together with other regulatory agencies ordered 13 of the largest technology firms to unbundle and restructure the internet-based businesses' financial businesses into licensed financial service providers.[133] With this move, the Chinese authorities can bring digital financial activities within the regulatory perimeter of financial regulation to "break [the] information monopoly" and "enhance the sense of social responsibility."[134] However, the explicit delegation of pseudo-public functions to major platforms (like the right of Alibaba to legally prosecute individuals and businesses breaching rules on its platform, or the total access of the Chinese government to company data) skews competition interests towards ensuring a thriving, yet protectionist internal market.[135] Though foreign internet users can access Chinese websites, those aiming to

131. For a discussion on China's state support to its private sector, see generally USHA C. V. HALEY & GEORGE T. HALEY, SUBSIDIES TO CHINESE INDUSTRY: STATE CAPITALISM, BUSINESS STRATEGY, AND TRADE POLICY (2013) (highlighting a trend in China to support local companies).

132. Paolo Beconcini, *International Challenges Help China and the EU Find Agreement on Technology Transfer*, NAT'L L. REV. (Jan. 14, 2021), https://www.natlawreview.com/article/international-challenges-help-china-and-eu-find-agreement-technology-transfer.

133. *See* Keith Zhai, *China Orders Tech Giants to Unbundle Financial Services*, WALL ST. J. (Apr. 30, 2021), http://www.wsj.com/articles/china-orders-tech-giants-to-unbundle-financial-services-11619780759. (the 13 firms include Tencent, Du Xiaoman Financial, JD Finance, ByteDance, Meituan Finance, DiDi Finance, Lufax, Airstar Digital Technology, 360 DigiTech, Sina Finance, Suning Finance, Gome Finance, and Ctrip Finance).

134. *Id.*

135. Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMP. INT'L DEV. 45, 46-54 (2021) (outlining concerted governance efforts to protect burgeoning digital markets); Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563, 1573-87 (2017) (highlighting a unique form of delegating administrative governance functions to digital platforms).

enter the Chinese market have little choice but to use Chinese platforms like Weibo. In part because of these mercantile and protectionist policies, in 2018 China accounted for 40 percent of the total revenue of the top ten digital trade operating countries.[136] Looking forward, these data capacities are being embedded and reinforced through a sophisticated Social Credit System that makes use of a centralized digital ID program and an experimental Digital Yuan initiative to interlink individuals, businesses, and social organizations.[137]

The variables characterizing each domestic style are consolidating into increasingly contrasting and, in many cases, conflicting data governance regimes. The result is a reversal of the data globalization process and a growing fragmentation of data flows and infrastructure. In fact, the findings of the style analysis (summarized in Table 1) indicate that the three major economies pursue uncooperative strategies to address shared policy concerns over national security, international competitiveness, and control over private actors. Furthermore, they adopt substantially different approaches to regulated ownership and control of data, emphasizing: property entitlements to support a market-based economy for data (the United States); consumers' rights to protect end-users (the European Union); and State centralization to pursue broader social and economic policies (China). Finally, from a practical standpoint, the mode in which domestic regulatory rules are designed and enforced differs substantially, with different reliance on the cooperation of regulated entities to implement regulatory regimes.

136. *See* Chu & Lee, *supra* note 129.

137. Jacqueline Hicks, *Digital ID Capitalism: How Emerging Economies are Re-inventing Digital Capitalism*, 26 CONTEMP. POL. 330, 330-50 (2020) (advancing an emerging digital ID-centric market).

Table 1. Governance Styles of the US, EU, and China: Key Variables

	Market Attitude			Guiding Principles			Regulatory Approaches	
	Variety of capitalism	*Policy priorities*	*Antitrust and competitiveness*	*Normative orientation*	*Personal data control/ mobility*	*Non-Personal Data control/ mobility*	*Mode of Regulation*	*Mode of Enforcement*
US	Liberal	Free market National security	Market efficiency	Property-based	Individual control established on contractual basis (with full alienability) Free data flow	Individual control established on contractual basis (with full alienability) Free data flow	Adversarial	Self-regulation
EU	Coordinated	Single Market creation and protection	Consumer-focused	Rights-based	Individual control (with non-alienable data) Restricted data flow	Individual control established on contractual basis (with full alienability) Free data flow	Outcome-based regulation	Enforced-self regulation
China	Organized	Cybersecurity Internal market development	Economic stability	State-based	State control (with non-alienable data) Restricted data flow	State control (with non-alienable data) Restricted data flow	Rule-based regulation	Command-and-Control

The consolidation of data governance styles and the emergence of competing and even conflicting data governance regimes has resulted in a fragmented transnational data governance framework. The consequences of this process are most clearly seen in the context of the global commons—a framework of institutional arrangements for the governance of globally shared resources among its stakeholders.[138] The internet, run on open source, non-exclusive and non-proprietary protocols is one such emergent global commons.[139]

138. Jennifer Shkabatur, *The Global Commons of Data*, 22 STAN. TECH. L. REV. 354 (2019) 383 (discussing how the data, utilizing the underpinning internet infrastructure, should be considered a global commons from a relational perspective).

139. *Id.*

III. FRAGMENTATION OF TRANSNATIONAL DATA GOVERNANCE: SOVEREIGNTY, COMPETITION, AND SECURITIZATION

Distinct data governance styles are evolving, which reflect different attitudes towards markets, policy priorities, principles, and regulatory approaches. Crucially, reactions to Big Tech's dominance have prompted initiatives to assert sovereignty over the digital world—first, in the European Union, then in China, and eventually in the United States. Over the past decade, concerns about data security have refocused on security (both individual and national) and competitiveness issues, as societies look to maximize the benefits of data for their own development while controlling risks of digitalization. The result is an international landscape where the three major economies compete to gain control and expand their influence over data and data flows.

Tensions and conflicting positions have become increasingly more apparent, besetting the process of data globalization that started three decades ago. The fracturing of the internet is the likely eventual result, as data can flow freely only within jurisdictional areas meeting potentially non-interoperable idiosyncratic requirements. At the global level, a new form of digital competition among major actors is emerging and is buttressed by the pursuit of digital (or data) sovereignty. To gain control, jurisdictions harden their stances, by exercising extraterritorial application of their laws, and by tightening access to and circulation of data for national security purposes.

This Section examines these dynamics, beginning with digital sovereignty as an emerging central priority. The process of data securitization highlights how the expansion of national security and defense policies is halting the process of data globalization. This can be seen most directly in the context of the impact on the internet, by identifying how conflicts beset the global data infrastructure.

A. DIGITAL SOVEREIGNTY

Digital sovereignty is an emerging concept with blurred contours.[140] Broadly, it refers to the level of control over data, infrastructure, and standards

140. On the different connotation of "digital sovereignty"—also referred to as "data sovereignty" or "cyber sovereignty"—see Patrik Hummel, Matthias Braun, Max Tretter & Peter Dabrock, *Data Sovereignty: A Review*, 8 BIG DATA & SOC'Y 1, 9-12 (2021) (providing a

held by a State vis-à-vis other States, private firms, and individual citizens.[141] It manifests as regulatory, legal, or technical control that state actors and private actors exercise, among and between them, over the digital world.[142]

Digital sovereignty also enables competition between data governance regimes. In fact, each jurisdiction seeks to expand its influence internally and externally by devising regulatory and technological solutions that can be adopted across the world. This phenomenon extends beyond traditional explanations for regulatory competition between jurisdictions. In the literature, it is often noted that market participants may choose to operate in different legal systems to maximize their revenues, thus spurring regulatory competition.[143] Studies have shown that this competition can have virtuous effects, pushing policymakers to devise more efficient rules in a race to the top where jurisdictions compete to design increasingly better rules, a phenomenon known as the "California effect."[144] Yet, negative consequences may surface

---

systematic review of data sovereignty studies, and highlighting the most common associations being with control and power, security, representation, and privacy); Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHIL. &. TECH. 369, 371 (2020) https://doi.org/10.1007/s13347-020-00423-6.

141. Alexandru Circiumaru, The EU's Digital Sovereignty—The Role of Artificial Intelligence and Competition Policy 1-10 (2021) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831815 (describing the three main characteristics of EU digital sovereignty as "autonomy, ability to influence, and protection of EU citizens' self-determination online").

142. Creemers, *supra* note 109 (proposing four dimensions to assesses digital sovereignty in any given jurisdiction: (i) the target of sovereignty and at whom the claim of sovereignty is aimed, (ii) the nature of the sovereignty claim in regard to the specific legal entitlements it constitutes, (iii) the objectives of the pursuit of sovereignty, and (iv) the means to realize sovereignty through legal-regulatory tools).

143. The concept of regulatory competition has been extensively examined since the 1950s, with the original analytical framework offered owed to Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416 (1956). Different models have been developed to explain regulatory rivalry and competitive dynamics within federal, supranational, or international markets for legal rules; *see* Claudio M. Radaelli, *The Puzzle of Regulatory Competition*, 24 J. PUB. POL'Y 23 (2004) (offering an overview and a critique of traditional models explaining regulatory competition).

144. Richard Perkins & Eric Neumayer, *Does the 'California Effect' Operate across Borders? Trading-and Investing-up in Automobile Emission Standards*, 19 J. EUR. PUB. POL'Y 217, 217-25 (2012) (using the example of automobile emission standards to find developing country automobile exports to countries with more stringent standards as a cause for more stringent standards in the exporting country); Dirk A. Heyen, *Influence of the EU Chemicals Regulation on the US Policy Reform Debate: Is a 'California Effect' within REACH?*, 2 TRANSNAT'L ENV'T L. 95,

when rules are relaxed to attract more market participants, thus, spurring a race to the bottom, also known as the "Delaware effect."[145] In the context of data governance, the competition between governance regimes cannot, at least in its current form, be encapsulated in this traditional dynamic. Domestic policymakers are concerned with expanding their sovereignty in the digital world vis-à-vis state and private actors alike.

Over the past several decades, the dominant liberal market approach to data and the internet has underpinned the evolution of the global data economy. Together with the first-mover advantage impetus reflected in the motto "move fast and break things,"[146] the American style of data governance became a model for most jurisdictions aiming at establishing a domestic Silicon Valley. As policymakers of different jurisdictions adopted a laissez-faire attitude towards data flows and data-intensive firms, the resulting process of data globalization reinforced the dominance of Big Tech. As the European Union began to set its own minimum rules for data governance in its internal market, it began to trigger the Brussels effect—as foreign companies trading in the Single Market had to adjust their conduct to fit the European Union's standards, the same companies are incentivized to lobby the standardization of such rules in their domicile nation-states.[147] While this was largely voluntary under the pre-GDPR approach of the 1995 Data Protection Directive (and widely adopted arguably as a reflection of the California effect of the attraction of the E.U. approach as an alternative to that of the United States), GDPR's data transfer rules are increasingly forcing the adoption of similar approaches

95-110 (2013) (finding the California effect from stringent E.U. chemicals standards to exported countries, but not to large trading partners like the United States).

145. The California and Delaware effects are two sides of the same conceptual coin and have been broadly discussed. *See* DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY 1-40 (2009) (introducing the concept of the California effect in an environmental rules contexts); Richard Perkins & Eric Neumayer, *Does the 'California Effect' Operate across Borders? Trading-and Investing-up in Automobile Emission Standards*, 19 J. EUR. PUB. POL'Y 217, 217-28 (2012) (presenting the trans-jurisdictional evidence of the California effect); Fernán Restrepo & Guhan Subramanian, *The Effect of Delaware Doctrine on Freezeout Structure & Outcomes: Evidence on the Unified Approach*, 5 HARV. BUS. L. REV. 205, 205-17 (2015) (discussing the Delaware effect in the context of buyouts).

146. Until recently, this was the internal motto of Facebook, according to its founder. *See* Drake Baer, *Mark Zuckerberg Explains Why Facebook Doesn't "Move Fast And Break Things" Anymore*, BUS. INSIDER, (May 2, 2014) https://www.businessinsider.com/mark-zuckerberg-on-facebooks-new-motto-2014-5.

147. *See* O'Hara, *supra* note 20.

elsewhere as a condition of digital access, reinforced by their extraterritorial application, bolstering the Brussels effect. This can be characterized as a liberal rights-based approach. China is also seeking growing influence under the Beijing effect, through which China is shaping transnational data governance through initiatives like the Digital Silk Road, whereby others are offered the tools to emulate China's state-centric, centralized form of data governance and control.[148] This is combined with a strategy of seeking to influence and lead the development and setting of technologies and technological standards, seen most widely in approaches to communications technologies and standards such as 5G and internet systems. Consequently, the competition between different strategies of digital sovereignty between the major economies leads to clashes between them.

1. Emerging Concepts

During the past decade, the exercise of sovereignty over the digital world has become a contentious area where governance styles began to collide. While the European Union has been *de facto* the first mover in enacting a cross-sectoral governance framework to curtail the level of control that firms can exercise over the personal data of individuals, the concept of digital sovereignty has been first used to assert the sovereign powers of nation-states. Specifically, reference to "sovereignty" appeared as a point of policy tension between the United States and China.[149] In 2010, following the U.S. "internet freedom agenda"—that extended the freedoms of expression, religious belief, and assembly of the physical world to the internet[150]—the Chinese government issued a White Paper in which the internet was defined as a sovereign space—

148. Marie Lamensch, *Authoritarianism Has Been Reinvented for the Digital Age*, CTR. FOR INT'L GOVERNANCE INNOVATION (JULY, 9, 2021), https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/; (outlining the development of digital authoritarianism and its characteristics); Erie & Streinz, *supra* note 31 (explaining the use of the Digital Silk Road and One Belt One Road investments as vehicles for transferring data governance approach).

149. Hillary Rodham Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

150. According to this vision, the internet was to be an "open, interoperable, secure, and reliable" information infrastructure. *See id.*

a matter of national security and public interests.[151] These ideational conceptions manifest in different, at times conflicting outputs.

Data sovereignty is evolving as a legal notion to reflect the variety of governance and capitalism embraced by each jurisdiction. As the point of origin of the world's data infrastructure and data economy, the United States has been promoting an open and global market economy for data where sovereignty has been primarily intended as a mechanism to empower market participants and also freedom of expression. The full control over data, exercised through the full alienability of ownership rights over data, has been a central tenet of the data economy that, from the United States, spread throughout a significant portion of the world.

Unlike the United States, the European Union has aimed at achieving digital autonomy to protect both a European rights-based society and the Single Market while supporting competitiveness vis-à-vis the United States and increasingly China.[152] Albeit the term is not deployed uniformly,[153] digital sovereignty has been outlined as a goal in the visions communicated by the European Commission's Roadmap for the Digital Decade.[154] Moreover, it has been reinforced as an objective by the European Council,[155] European

151. *The Internet in China*, STATE COUNCIL INFO. OFF. (China) (June 8, 2010) http://hk.ocmfa.gov.cn/eng/jbwzlm/xwdt/zt/zfbps/201206/t20120621_10095576.htm.

152. The European Union Agency for Cybersecurity (ENISA) defines digital strategic autonomy as "the ability of Europe to source products and services that meet its needs and values, without undue influence from the outside world." *See* EUR. UNION AGENCY FOR CYBERSECURITY (ENISA), CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU'S DIGITAL STRATEGIC AUTONOMY (Apr. 23, 2021), https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy.

153. *See* Circiumaru, *supra* note 141.

154. EUR. COMM'N, EUROPE'S DIGITAL DECADE: 2030 DIGITAL TARGETS (2021), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12900-Europe-s-digital-decade-2030-digital-targets; *See also 2030 Digital Compass: the European way for the Digital Decade*, COM (2021) 118 final (Sept. 3, 2021).

155. GER. PRESIDENCY OF THE COUNCIL OF THE EUR. UNION, TOGETHER FOR EUROPE'S RECOVERY (2020), https://www.eu2020.de/blob/2360248/e0312c50f910931819ab67f630d15b2f/06-30-pdf-programm-en-data.pdf; Charles Michel, President of the Eur. Council, Digital Sovereignty is Central to European Strategic Autonomy (Feb. 3, 2021) https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

Parliament,[156] the European Union Agency for Cybersecurity (ENISA),[157] and the individual Member States.[158]

Of the three major economies, China has advanced the clearest and broadest position on digital sovereignty. In 2017, China released the International Strategy of Cooperation on Cyberspace, highlighting "cyber sovereignty" in the context of extending State-based controls to the digital realm. In such a document, China recognizes the sovereign rights of the national government vis-à-vis other governments, non-state actors, and equality of states via multilateral state-led management of the digital realm versus the current decentralized model.[159] From this general principle flows three objectives:[160] (1) the maintenance of control over the flow of information to preserve the country's stability; (2) the establishment of technological autonomy; and (3) the creation of a digital realm where the country's military, political, and economic influence is reflected.

2. Divergent Scopes

Digital sovereignty is a central aspect of shaping data governance regimes. In the United States, historically, digital sovereignty has asserted the primacy of private firms, limited only by national security interests. For example, in 2018, the U.S. Federal Communications Commission reclassified internet service providers as information services instead of common carrier services, thus removing net neutrality rules in the United States—allowing ISPs to assign different speeds to different user data flows.[161] Yet, in line with the adversarial nature of the U.S. modality of regulation, efforts of federal agencies to control the internet have been curtailed by courts. Law enforcement

156. Tambiama Madiega, *Digital sovereignty for Europe*, EPRS IDEAS PAPER (July 2020) https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

157. *See* ENISA, *supra* note 152.

158. In 2016, Germany and France promoted European digital sovereignty in the Franco-German Council of Ministers. Press Release, Nat'l Cybersecurity Agency of Fr. (ANSSI), The European digital sovereignty –A common objective for France and Germany (Apr. 7, 2016) https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/.

159. INTERNATIONAL STRATEGY OF COOPERATION ON CYBERSPACE (Mar. 08, 2017), http://p.china.org.cn/2017-03/08/content_50081017_3.htm (China).

160. *See* Creemers, *supra* note 109.

161. State rules, however, can supersede the federal rules, though so far only California is enforcing net neutrality.

agencies have tried to seize domain names, in application of the Pro IP Act, allowing the federal government to take control of property suspected of being used in criminal activity.[162] However, courts have limited this interpretation that would have allowed them to take down websites based on summary evidence of criminal activities.[163] This approach is now clearly evolving under both the Trump and Biden administrations, but as yet with no clear path other than competing with China, maintaining U.S. power, and reducing the power of Big Tech.

In contrast, the European Union aims at protecting consumers, thus, interpreting sovereignty as a system of rights that justifies public intervention in the digital world, like in any other market. Through this prism, the 2017 Consumer Protection Regulation expressly provides regulators within the European Union authority to block ISPs, web hosts, domain registries, and delete websites, even if they are not European.[164] In line with its outcome-based regulatory mode, the European Union intends to incentivize online platforms to align with European values when it comes to business conduct and behavior towards society, as highlighted by the upcoming Digital Services Act package that requires transparency about how online platforms influence user activity.[165] In the European Union, net neutrality is laid down by E.U. Regulation 2015/2120: Safeguarding of open internet access, which is an integral part of the Union's Digital Single Market policy.[166] The law ensures a minimum level of net neutrality in the European Union (and, more broadly in the European Economic Area). However, it also allows for the Member States

162. Specifically, The Pro IP Act 18 U.S.C. §§ 2323. *See generally* Karen Kopel, *Operation Seizing Our Sites: How the Federal Government is Taking Domain Names without Prior Notice*, 28 BERKELEY TECH. L.J. 859, 860-77 (2013) (discussing a trend of US seizures of domain names by the Immigration and Customs Enforcement Office to protect intellectual property rights).

163. Puerto 80 Projs. v. United States, Case 1:11-cv-04139-PAC (S.D.N.Y., 4 Aug. 2011) (order denying petition for release of domain names seized by Immigration and Customs Enforcement).

164. *The Internet and Extra-Territorial Effects of Laws*, INTERNET SOC'Y (Oct. 18, 2018), https://www.internetsociety.org/resources/doc/2018/the-internet-and-extra-territorial-effects-of-laws/.

165. *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Service Act) and amending Directive 2000/31/EC 2020*, COM (2020) 825 final (Dec. 15, 2020).

166. *See* Harald Øverby & Jan A. Audestad, Standards, Regulations, and Net Neutrality in the Digital Economy 26 (May 15, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3601725 (finding net neutrality and other standards as increasingly powerful representatives of regulatory trajectories).

to specify stricter neutrality requirements, allowing the prioritization of specialized services like remote surgery or driverless cars.[167]

Finally, China displays a state-centered focus supported by a command-and-control approach. Domestic sovereignty over data and data infrastructure is highly centralized and supported by precise rules with limited room for interpretation by market participants. Concretely, this governance regime works through a combination of regulatory provisions and technological solutions implemented to manage data flows, access and uses within the Great Firewall.[168] Regulators can request private companies to immediately hand over necessary data or block contents.[169] Circumvention technologies, like virtual private networks, are actively interrupted and the government can disconnect companies or whole regions from the internet as necessary.[170]

Though Chinese ISPs are not neutral in monitoring and reacting to politically harmful information, commercial network neutrality is becoming a growing policy priority.[171] Similarly, there have been ongoing discussions to open cross-border data flows. The Data Security Law stipulates that the government will actively engage and promote ". . . the secure and free flow of data across borders."[172] This has been reflected in policy documents denoting the establishment of the Hainan Free Trade Port, with a pilot for more liberal

167. *Id.*

168. *See* JAMES GRIFFITHS, THE GREAT FIREWALL OF CHINA: HOW TO BUILD AND CONTROL AN ALTERNATIVE VERSION OF THE INTERNET 22-64 (2019) (investigating examples of how the firewall has been employed on the internet for state purposes).

169. This was for instance the case for WeChat and Weibo, two popular messaging services and social networks. *See* Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace*, NAT'L BUREAU ASIAN RSCH. No. 87 (2020).

170. *See* GRIFFITHS, *supra* note 168.

171. Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration*, 207 CHINA Q. 523, 523-29 (2011) (discussing the phenomenon of network convergence in the form of growing ISP service standardization in China); Jun Wu & Qingqing Wan, *From Wechat to We Fight: Tencent and China Mobile's Dilemma*, PAC. ASIA CONF. ON INFO. SYS. 265, 265–75 (2014) (while there is a high level of state intervention in data governance, there is still a level of self-regulation in the Chinese market, especially when outside the scope of data content); Meijuan Li & Lei Hou, *Welfare Effects of Network Neutrality in Mobile Internet Market*, 14 ENTER. INFO. SYS. 352, 352-55 (2020) (arguing that net neutrality should be enforced in China for the economic welfare gains).

172. *China's Data Security Law Will Create Dilemmas*, OXFORD ANALYTICA (Aug. 5, 2020), https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB254376/full/html; Creemers, *supra* note 109.

cross-border data flows,[173] or the Shanghai municipal guideline which aims to relax restrictions and generate increasing white lists of companies with direct access to the "international internet."[174] An example of the free flow of data is the growing connection of banks serving Chinese state-owned enterprises and corporations to the global SWIFT payment messaging networks. At the same time, recent changes mandate both data localization and monitoring of any cross-border flows.[175]

In addition, as evidenced by the approach adopted in the European Union and China, digital sovereignty is not limited to asserting control over data and data flows. It also implies the establishment of technological and infrastructural independence. Both jurisdictions aim to reduce (E.U.) or eliminate (China) dependence on U.S. companies and technology. To manage data in the Single Market, the European Union has launched the European Cloud Initiative, to simplify access to data by making it possible to move, share and reuse data seamlessly across European markets and borders.[176] Together with the Franco-German GAIA-X, initiative—a project to connect cloud providers around Europe, harmonize technical standards, and ensure data privacy and security walls—the European Union is creating its own walled garden of data.[177] Federated cloud initiatives are also at the base of ensuring commitment to E.U. values, most recently enshrined in the Berlin Declaration on Digital Society and Value-Based Digital Government.[178] These initiatives reflect the wider strategy to build a secure, high-quality, competitive digital

173. *The Central Committee of the Communist Party of China and the State Council Issued the "Overall Plan for the Construction of Hainan Free Trade Port,"* XINHUA NEWS AGENCY (June 1, 2020), http://www.xinhuanet.com/politics/2020-06/01/c_1126061034.htm.

174. Xiaomeng Lu, *Is China Changing Its Thinking on Data Localization?*, THE DIPLOMAT (June 4, 2020), https://thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/.

175. China's cyberspace regulator recently launched an investigation into one of China's largest tech companies over an alleged failure to follow personal data collection rules. Josh Horwitz & Yilei Sun, *Explainer: What is Driving China's Clampdown on Didi and Data Security?*, REUTERS (July 7, 2021) https://www.reuters.com/technology/what-is-driving-chinas-clampdown-didi-data-security-2021-07-07/.

176. *Cloud Computing*, EUR. COMM'N, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing (last visited Mar. 29, 2021).

177. Konstantinos Komaitis, *Europe's Ambition for Digital Sovereignty Must Not Undermine the Internet's Values*, 2021 COMPUT. FRAUD & SEC. 11, 12-16 (2021) (arguing that the internet needs to be retrofitted for modern emerging legal problems).

178. *Berlin Declaration on Digital Society and Value-Based Digital Government*, EUR. COMM'N (Dec. 8, 2020), https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government.

infrastructure, without relying on U.S. companies or Chinese data infrastructure vendors.[179]

China aims to reduce and ideally eliminate dependence on foreign entities for handling data, as well as providing data infrastructure. A draft measure by the China Banking Regulatory Commission in 2014 called for three-quarters of ICT products in China's banking system to be "secure and controllable" by 2019.[180] The same year, the Chinese government ordered every government office and public institution to remove all foreign software and hardware within the next three years.[181] These measures have become explicit in 2020 and 2021 as the result of the new Data Security Law, PIPL, State Council strategy, and other changes appearing to set out an increasingly autarkical trajectory, albeit one which permits and even encourages others to join.

B. EXTRATERRITORIALIZATION AND INTERNALIZATION

In addition to its function of regulating public-private relationships internally, digital sovereignty seeks to support and protect domestic interests in the international arena. This occurs in two manners.

First, through the extraterritorial enforcement of domestic laws, states ensure the application of domestic policies outside jurisdictional borders. Although domestic governance styles may shape the mode of enforcement, extraterritorial application of domestic regimes is essential in the context of data mobility. In 2014, Microsoft challenged an FBI warrant to surrender the

---

179. Ulrike Franke Torreblanca Carla Hobbs, Janka Oertel, Jeremy Shapiro & José Ignacio, *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry—European Council on Foreign Relations*, EUR. COUNCIL ON FOR. REL. (July 30, 2020), https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

180. Zhōngguó yínháng yè jiāndū guǎnlǐ wěiyuánhuì guānyú yìngyòng ānquán kě kòng xìnxī jìshù jiāqiáng yínháng yè wǎngluò ānquán hé xìnxī huà jiànshè de zhǐdǎo yìjiàn (中国银行业监督管理委员会关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见) [Guiding Opinions on Applying Secure and Controllable Information Technologies to Strengthen the Cybersecurity and Informatization Construction of the Banking Industry], CHINESE BANKING REGULATORY COMMISSION (Sept. 3, 2014), *translated in* DIGICHINA: STANFORD UNIVERSITY (Sept. 3, 2014), https://digichina.stanford.edu/work/guiding-opinions-concerning-using-secure-and-controllable-information-technology-and-strengthening-cybersecurity-and-informatization-in-the-banking-sector/.

181. Yuan Yang & Nian Liu, *Beijing Orders State Offices to Replace Foreign PCs and Software*, https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406 (last visited Jan. 16, 2023).

emails of a target account stored on a server located in Ireland, claiming that the warrant has no extraterritorial reach.[182] As the U.S. Court of Appeals for the Second Circuit ruled in favor of Microsoft, the Department of Justice filed an appeal with the Supreme Court in 2017, arguing that because Microsoft employees could access the data, they must comply with the warrant.[183] The case was mooted when Congress introduced the CLOUD Act, allowing enforcement agencies to compel the production of communications content without regard to the location of the data.[184] Beyond the new authority granted by the CLOUD Act, extraterritorial sovereignty is exercised in other areas of data governance. For instance, courts have required internet search engines, web hosting sites, internet service providers, and domain name registries to cease facilitating access to certain content based on IP infringement.[185]

The European Union has likewise taken an explicitly extraterritorial approach in recent years, as the GDPR establishes a set of rules for personal data within and outside of the European Union. In particular, unless provided equivalent protections to the data of citizens held inside the European Union, data mobility and related economic activities with the Single Market are prohibited. Moreover, the 2013 Directive on Attacks Against Information Systems extends the notion of a criminal act to the territory where the offense occurs and imparts extraterritorial jurisdiction based on the active nationality principle.[186] The principle applies a jurisdiction's criminal laws to the conduct of its citizen outside the jurisdiction's borders, thereby ensuring extraterritoriality in cybersecurity. Through these initiatives, the European Union also aims to set the standard for the treatment of data, since the implementation of a minimum level of E.U. standards is a precondition to deal with E.U. citizens' personal data.

---

182. The warrant was provided to the FBI on the basis of the Stored Communications Act. *See* 18 U.S.C. §§ 2701-2712.

183. *See* Microsoft Corp. v. United States, 829 F.3d 197, 216 (2d Cir. 2016) (concluding "that Congress did not intend the [Stored Communications Act's] warrant provisions to apply extraterritorially").

184. *See* Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348, div. V (2018) (codified in scattered sections of 18 U.S.C.)

185. *See, e.g.*, Elsevier Inc. v. www.Sci-Hub.org, 2015 WL 6657363, at *1 (S.D.N.Y. Oct. 30, 2015) (where a judgment prescribed extraterritorial reach of the Copyright Act of 1976, by requiring injunctions of content against alien defendants). For a discussion of the extraterritorial reach, see Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9 (2018-2019).

186. *See* INTERNET SOC'Y, *supra* note 164.

Like the United States, China has also established rules authorizing the unilateral extraction of data concerning legal or natural persons being investigated under Chinese criminal law from servers and hard drives located outside of China.[187] Law enforcement agencies are granted the power to extract data via the internet and have established remote network inspection standards to detect criminal activities.[188]

Second, sovereignty supports policies aimed at protecting states from internal and external threats. With mounting geopolitical competition, particularly between the United States and China, digital sovereignty has been taking a national security and intelligence character. In more recent years, the U.S. State Department and the Department of Defense formulated the International Strategy for Cyberspace and the Strategy for Operation in Cyberspace in 2011, which set principles for the formation of cyber-alliances and containment of malicious behavior in cyberspace.[189] The U.S. national defense strategy proclaims a "right to self-defense" in cyberspace, explicitly declaring the capability to block or control conflict escalation through network methods as a strategic objective.[190] An expanding policy lexicon imparts the cyber domain with a spatial status similar to that of land, sea, air, and space doctrine, encompassing a need to secure "a freedom of action" in the space, which has a binary inside/outside character.[191] Through the Foreign

187. Guānyú bànlǐ xíngshì ànjiàn shōují tíqǔ hé shěnchá pànduàn diànzǐ shùjù ruògān wèntí de guīdìng [关于办理刑事案件收集提取和审查判断电子数据若干问题的规定] (Provisions on Several Issues Concerning the Collection, Extraction, Examination and Judgment of Electronic Data in Handling Criminal Cases) (promulgated by the Sup. People's Ct., Sup. People's Proc., and Ministry of Pub. Sec., 2016, effective Sept. 20, 2016) Art. 9 https://www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml (providing for "inspection" of a remote computer information system through the network in case the original storage medium cannot be seized) *translated in* CHINA LAW TRANSLATE (Sept. 20, 2016), https://www.chinalawtranslate.com/en/provision-on-collection-and-review-of-digital-information-in-criminal-cases/.

188. *Id.* Remote network inspections on remote computer information systems related to crime include: investigation, discovery, and collection of electronic data through the internet.

189. EXEC. OFF. OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD, (2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

190. *Id.* at 9.

191. *See* Jordan Branch, *What's in a Name? Metaphors and Cybersecurity*, 75 INT'L ORG. 39, 41-55 (2021) (proposing that foundational metaphors in digital governance are highlighting paradigmatic shifts towards controlling cyberspace).

Intelligence Surveillance Act (FISA), the NSA (National Security Agency) is authorized to perform electronic surveillance of foreign intelligence without warrant.[192] In light of its supranational character, the European Union is limited to a coordinating role in national security matters. While it protects E.U. citizen data from potential surveillance by third countries, as found in the *Schrems II* decision,[193] the European Union does not prohibit the cyber operations of Member States—which remain outside the E.U. mandate.[194] In China, Cybersecurity Law protects national interests in the digital space. The Cyberspace Administration of China has, for example, enacted regulations banning "fabricating information or inciting extreme emotions" in public internet accounts—regardless of whether the internet account is on a local or extraterritorial website.[195]

The assertion of digital sovereignty to defend against internal and external threats supports the growing expansion of national security and defense policies in the digital world. As datafication continues, fewer and fewer sectors remain digitally independent from others. Societal dependencies on digital systems, including the digital economy, public sphere, critical industrial infrastructure, democratic and other governance processes, and even day-to-day societal functions are contingent on digital security.[196] In turn, human and national security are increasingly dependent on the authenticity, availability, integrity, and confidentiality of data.[197] Securing and maintaining control over data, data flows, and data infrastructure are critical for a wide range of policies and to support fundamental societal functions. However, absent an

192. 50 U.S.C. § 1881.

193. Case C-311/18 Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2019:1145 (July 16, 2020).

194. *See* Theodore Christakis, *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)*, EUR. L. BLOG (Apr. 13, 2021), https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/.

195. 互联网用户公众账号信息服务管理规定 [Hùliánwǎng yònghù gōngzhòng zhànghào xìnxī fúwù guǎnlǐ guiding] (Administrative provisions on the Information Services Provided through Official Accounts of Internet Users) (promulgated by the Cyberspace Administration of China, Jan. 22, 2021, effective Feb. 22, 2021) http://www.cac.gov.cn/2021-01/22/c_1612887880656609.htm *translated in* CHINA LAWS PORTAL (Jan. 22, 2021), https://www.chinajusticeobserver.com/law/x/administrative-provisions-on-the-information-services-provided-through-official-accounts-of-internet-users-20210122

196. *See* DENARDIS, *supra* note 6, at 131.

197. *See* DENARDIS, *supra* note 6, at 131.

internationally concerted approach, the jurisdictional securitization of data governance further deepens fractures.

C. DATA SECURITIZATION

Data securitization is a process whereby jurisdictions absorb data governance, or a significant portion of it, within the perimeter of national security and defense policies. The intensity of securitization is scalar rather than binary. In some cases, jurisdictions made exceptional provisions to control the use of data and protect national interests in case of external or internal threats. An example is the "right to self-defense," set out in the U.S. International Strategy for Cyberspace.[198] In other instances, security concerns permeate domestic data governance. In China, the Cybersecurity Law is a constitutive component of the country's emerging data governance regime; in the United States, FISA allows the NSA to collect information from foreign firms.[199] Data securitization is, therefore, a process that occurs irrespective of the level of liberalism towards data governance.[200] Crucially, steps towards greater securitization of data in one jurisdiction trigger counteractions in others, fueling a progressive absorption of data governance into national security and defense policies. The spatial metaphors to support American cybersecurity, [201] for example, naturalize the existence of threats and subsequently legitimize reactions, such as the tightening of the controls through the Great Firewall, in China. Interjurisdictional tensions, and interstate cooperation (with allies), are intensifying, thus deepening the fragmentation of global data governance and pushing the formation of "digital Berlin walls."[202]

198. *See* Lu *supra* note 174.

199. 50 U.S.C. § 1881.

200. Thierry Balzacq, Stefano Guzzini, Michael C. Williams, Ole Wæver & Heikki Patomäki, *What Kind of Theory—If Any—Is Securitization?*, 29 INT'L REL. 96 (2014) (presenting the emerging theory of securitization across various disciplines); Maximiliano Facundo Vila Seoane, *Data Securitisation: The Challenges of Data Sovereignty in India*, 42 THIRD WORLD Q. 1733 (2021) (Using the Indian data governance regime as an example of securitization); Christian Kaunert & Sarah Léonard, *The Collective Securitisation of Terrorism in the European Union*, 42 W. EUR. POL. 261 (2019) (highlighting securitization in the European Union through a case study of counter-terrorism related regulatory efforts).

201. 50 U.S.C. § 1881.

202. Press Release, The White House, The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China (July 19, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/

In general terms, data securitization processes are evolving along two trajectories. In some cases, policymakers expand the scope of national security rules to include areas that are not traditionally related to national security matters. As the targets of cyber threats extend to a wider variety of organizations and economic actors,[203] so do the parameters of domestic cyber-resilience strategies that now include *inter alia* commerce, communications, individual privacy, finance, and intellectual property.[204] As a consequence, intelligence agencies increasingly rely on private sector participants to support their activities. For example, the U.S. PRISM surveillance program secured direct access to communication and stored information from the servers of Microsoft, Yahoo, Google, and Facebook.[205] In line with this trajectory, jurisdictions have designed holistic defense strategies that include the digital world.[206] The European Union has advanced a comprehensive data securitization package starting with the Cybersecurity Strategy, which coalesces a variety of rules and includes supranational and national intelligence agencies,

2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

203. More than seventy percent of all global companies and organizations are estimated to be subject to virtual attacks, and their frequency is increasing by approximately forty percent every year, with cascading and unpredictable consequences. *See* WORLD ECON. F. CTR. FOR CYBERSECURITY, ANNUAL GATHERING OF THE CENTRE FOR CYBERSECURITY COMMITTED TO SECURING OUR SHARED DIGITAL FUTURE (2018). For more general discussion on cybersecurity, see NortonLifeLock, *2019 Cyber Safety Insights Report Global Results* (Mar. 30, 2020) (discussing a notable example of cybersecurity risks being the hack of SolarWinds, in 2020 provided hackers access to the data of Fortune 500 companies).

204. For example, the U.S. National Cyber Strategy aims to identify critical function lists that are sensitive to cybersecurity, including national security, energy and power, banking and finance, health and safety, communications, information technology, and transport. THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (2018).

205. For a discussion of the U.S. PRISM program, see generally Alex Marthews & Catherine E. Tucker, Government Surveillance and Internet Search Behavior (Mar. 15, 2017) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564; Genna Churches & Monika Zalnieriute, *'Contracting Out' Human Rights in International Law: Schrems II and the Fundamental Flaws of US Surveillance Law*, HARV. INT'L L.J. ONLINE (2020), (discussing how the EU Courts found surveillance programs like PRISM, that collected data directly from undersea cables and providers like Google and Facebook, were necessary for foreign intelligence).

206. *See* Chooi Shi Teoh & Ahmad Kamil Mahmood, *National Cyber Security Strategies for Digital Economy*, INT'L CONF. ON RSCH. & INNOVATION IN INFO. SYS. (ICRIIS) 1-9 (2017) (discussing the growth of cybersecurity regulation).

law enforcement, defense authorities, and industry stakeholders.[207] Within this framework, the European Union established a minimum set of security standards.[208] Furthermore, current proposals entail a pan-E.U. authority, the ENISA, with the mandate to increase operational cooperation between the Member States of the European Union and to establish a European cybersecurity certification framework to assess the risks of digital products and services.[209]

A second policy trajectory departs from the national security and defense paradigm and mandates the implementation of data security systems to private entities for consumer protection.[210] Cybersecurity provisions are embedded in sector-specific regulatory frameworks. The rules concerning privacy and data protection in the financial sector epitomize this trajectory. The Gramm-Leach-Bliley Act of 1999 compels financial institutions to implement data security requirements to safeguard "security and confidentiality" of customers' records and to protect their systems from unauthorized access.[211] Similarly, in the European Union, the regulatory framework for financial services comprises a

207. Anton Didenko, *Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonisation in the EU and Beyond*, 25 UNIFORM L. REV. 125, 125-35 (2020) (presenting an emergence of cybersecurity regimes in all three jurisdictions discussed in this paper).

208. The Security of Network and Information System (NIS) Directive establishes a baseline that can be overridden by other sectoral rules. *See* Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) /1.

209. The instrument was adopted in its final form in April 2019. *See* Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019 O.J. (L 151) /15.

210. *See* Zachariah Tyree, Robert A. Bridges, Frank L. Combs & Michael R. Moore, *Exploiting the Shape of CAN Data for In-Vehicle Intrusion Detection*, 2018 IEEE 88TH VEHICULAR TECHNOLOGY CONFERENCE (VTC-FALL) 1 (2018). Jake L. Beavers, Michael Faulks and Jims Marchang, *Hacking NHS Pacemakers: A Feasibility Study*, 2019 IEEE 12TH INTERNATIONAL CONFERENCE ON GLOBAL SECURITY, SAFETY AND SUSTAINABILITY (ICGS3) 206 (2019).

211. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.). Additional rules may be applicable, depending on the state. *See, e.g.,* New York Financial Cybersecurity Regulation, N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017). (requiring inter alia for financial institutions to implement "defensive infrastructure" to protect their ITC systems). For an analysis of the regulation, see Jeff Kosseff, *New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model*, 1 GEO. L. TECH. REV. 432 (2016) (arguing that the New York regulation is a model cybersecurity statute for the United States because it provides an industry-neutral framework).

burgeoning cybersecurity framework, led by the proposal of the Digital Operational Resilience Act, which introduces standardization of security measures, resilience testing, and cross-border cybersecurity oversight for banks in the Union.[212]

Cybersecurity is a threat to individual state security and digital sovereignty that also impacts the common global data infrastructure. Tensions between individual state objectives and the global commons are increasingly evident, with the potential to result in its fragmentation and fracture.

D. THE END OF THE INTERNET AS A GLOBAL COMMONS?

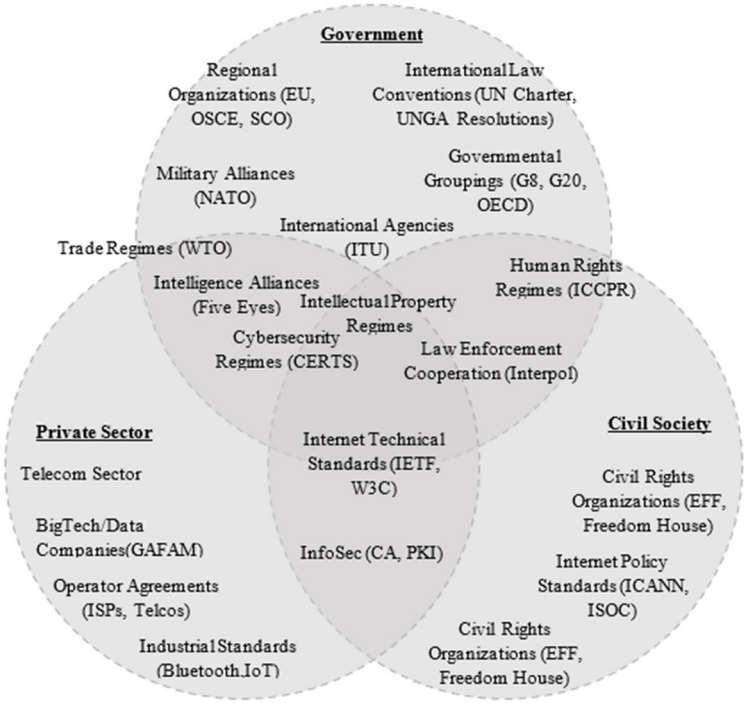
The internet is a network of networks through which most data travels around the world. It is a global commons that connects billions of data-dependent devices into a virtual economy that by itself is among the largest in the world.[213] The internet is the lifeline for everything from sending emails, to enabling whole sectors of the global economy, like finance or trade. The incumbent liberal model of the internet is the result of a wide international cyber "Internet Regime Complex"—an interconnected network of international regimes that, through their independent functions, prop up a liberal, permission-less, and open internet.[214]

212. Proposal for a Regulation of The European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM (2020) 595 final (Sept. 24, 2020).

213. The internet has developed the World Wide Web and its superstructural market through a variety of technological advances. *See* Christian Bizer, Tom Heath & Tim Berners-Lee, *Linked Data: The Story so Far*, *in* SEMANTIC SERVICES, INTEROPERABILITY & WEB APPLICATIONS: EMERGING CONCEPTS 205, 205-21 (2011) (discussing the "Linked Data" that has fostered a revolution in data access and utility); Tim Berners-Lee, James Hendler and Ora Lassila, *The Semantic Web*, 284 SCI. AM. 34 (2001) (presenting the idea of the "Semantic Web" in which data is linked by semantic logic); NAT'L AUDIT OFF., THE UK CYBER SECURITY STRATEGY: LANDSCAPE REVIEW (Feb. 12, 2013) (highlighting that the internet underpins an economy that by itself is in the top five globally).

214. *See* Nye, *supra* note 42.

Figure 1: The Internet Regime Complex[215]



The Internet Regime Complex consists of many separate, yet interlocking governance processes that together define the dimensions of the internet. The private sector provides most of the infrastructure and process data flows across the internet, while major decisions are taken at a government level, with the input of civil society for policy standards. The United States has been instrumental in creating this dynamic. The liberal market nature of the internet, for example, stems directly from the internet's construction upon the U.S. telecommunications regime, which the United States liberalized first domestically and then externally through the General Agreement on Trade in Services (GATS) and other Free Trade Agreements of the World Trade Organization (WTO).[216] As a consequence, in the incumbent "regime

215. Figure 1 is based on the following works. *See* Nye, *supra* note 42; Alexander Klimburg & Louk Faesen, *A Balance of Power in Cyberspace*, GOVERNING CYBERSPACE 145, 154 (2020) (promoting a three-part division of internet governance).

216. For a historical perspective on the globalization of telecommunications and the internet, see generally *The Changing Role for Telecommunications in the Economy: Globalisation and Its*

complex," the role of civil society and other governments in the role of the internet has been limited to technical and soft standards. However, as the U.S.-guided incumbent complex fractures, its derivative model of a unitary internet is similarly fragmenting.

The increasing territorialization of digital space via demarcations of digital sovereignty and data mobility is opening the possibility of a more fundamental fragmentation of the internet, and depletion of the global utility it brings. These dynamics are reflected in the emergence of a multi-centered internet where conflicts permeate each layer of the digital infrastructure.

1. A Multi-Centered Internet

While actors, principles, and regulatory approaches define distinctive governance styles, local capabilities have traditionally contributed to the development of the internet at different paces. Cyberspaces have historically been characterized by a center-periphery dynamic, where the United States and (to a lesser extent) Europe have benefited from first-mover advantages, while the South has lagged. The geographical distribution of internet users has been a key factor in the origins of this imbalance, with China experiencing relatively low internet penetration until the early 2000s.[217] A second factor is represented by the level of development in core infrastructure supporting data flow, with the United States initially significantly more advanced and branching to other continents, particularly Europe, through submarine cables.[218] Finally, the center-periphery imbalance has been heightened by the concentration in the United States and the European Union of companies engaged in activities that are essential to support the internet, such as the domain name system (DNS) and related servers, which are responsible for routing traffic to specific addresses and websites.[219] Having the ability to edit the DNS root, these

Impact on National Telecommunication Policy, OECD DIGIT. ECON. PAPERS NO. 11 (1995); DEREGULATION AND INTERDEPENDENCE IN THE ASIA-PACIFIC REGION 415–36 (Takatoshi Itō & Anne O. Krueger eds., 2000).

217. Max Roser, Hannah Ritchie & Esteban Ortiz-Ospina, *Internet*, OUR WORLD IN DATA (2015) https://ourworldindata.org/internet (highlighting that by 2005, the United States had seven times more internet users than China).

218. Dwayne Winseck, *Internet Infrastructure and the Persistent Myth of U.S. Hegemony*, *in* INFO., TECH. & CONTROL IN A CHANGING WORLD: UNDERSTANDING POWER STRUCTURES IN THE 21ST CENTURY 228-60 (2019) (highlighting that there is a relative decline of U.S. hegemony in internet infrastructure from half in 2004, to just twenty-five percent in 2017).

219. The majority of such infrastructure is still dominated by a handful of companies in the United States and Europe. *See generally*, Scott P. Sonbuchner, *Master of Your Domain: Should*

private entities effectively gained the power to remove a nation's internet presence completely while setting the terms of use for accessing the network.[220] Each of these factors resulted in disparities in internet capacity, leaving jurisdictions among the European Union and, to an even greater extent, China, as latecomers with limited influence in the early days of global information technology networks. These imbalances, however, sowed the seed for current fractures.

Recent efforts in China and the European Union to bolster digital infrastructure are seeking to redress, at least partially, the center-periphery dynamic. Yet, as both E.U. and Chinese infrastructure enhancements are occurring with the primary aim of developing an internal market, the center-periphery imbalance is morphing into a multi-centered internet structure with new peripheries. Each major jurisdiction represents a new center, equipped with the adequate infrastructural capacity and a distinctive governance approach. Each center competes to expand its sphere of influence, maximize the benefit of the data economy, and assert sovereignty and influence.

2. Data Infrastructure Conflicts

From an analytical standpoint, the internet is a data infrastructure comprising three layers, as suggested in the Benkler-Lessig model: (1) the physical infrastructure layer; (2) the code layer; and (3) the content layer.[221] The infrastructure layer forms the physical objects and comprises infrastructures that enable transnational data flows and that collect, store, and process data.[222] This layer links the physical and digital worlds through wires, cables, spectrum, and hardware like computers or routers.[223] Over 400 fiber-optic submarine cables, myriad microwave devices emitting wireless 4G and 5G, thousands of satellites, balloons, and unmanned aerial vehicles provide access to the internet

the US Government Maintain Control over the Internet's Root, 17 MINN. J. INT'L L. 183 (2008). (arguing that while the Internet Corporation for Assigned Names and Numbers was a semi-private nonprofit organization in California, the US could ensure physical control over internet routing).

220. *Id.*

221. Lawrence Lessig, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 23-25 (2002).

222. *Id.*

223. *Id.*

across the globe.[224] The second layer encompasses software for the carriage, storage, and delivery of data.[225] It comprises both lower-level software for the carriage, storage, and delivery of data (like the TCP/IP protocol), and higher-level software like operating systems. The content layer encompasses a semantic input that is understandable by end-users via all the materials stored, transmitted, and accessed using the software tools of the previous layer.[226]

To ensure cross-border digital connectivity, allowing data flows to move outside domestic borders, there must be a minimum level of harmonization of infrastructures and technical standards.[227] Yet, current trends include the decoupling and the duplication of technological infrastructures, the definition of different technical standards, and the compartmentalization of contents within domestic borders as a result of the emergence of competing, non-interoperable, and increasingly conflicting data governance regimes across major economies, combined with their external export, resulting in fragmentation of transnational data governance. These dynamics reflect profound conflicts that can be observed in each layer of the data infrastructure.

In the first layer (physical infrastructure), the vast majority of infrastructure, like submarine cables, has historically been laid by companies domiciled in the United States. Concurrently, the United States led the creation of regulatory standards for the use and access of the infrastructure, reflecting its open-market policy focus exemplified by the GATS Telecommunications Reference Paper and Agreement on Basic Telecommunications.[228] Together, these documents set out the principles of universal service, licensing, and allocation—stressing, in particular, market access to telecommunications for foreign market participants.[229]

These premises and the resulting transnational data governance framework are being challenged by both the European Union and China. The European

224. *See* L. Chettri & R. Bera, *A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems*, 7 IEEE INTERNET THINGS J. 16, 16-20 (2020) (describing the development of wireless systems).

225. *Id.*

226. *Id.*

227. Pau Puig Gabarró, DIGITAL CONNECTIVITY (2020).

228. Kirsten Rodine-Hardy, *Globalization, International Organizations, and Telecommunications: Globalization, International Organizations, and Telecommunications*, 32 REV. POL'Y RSCH. 517 (2015). (discussing the convergence of the main global telecommunications rules and their adherence to the free market model).

229. *Id.*

Union has taken the upgrade of the existing framework as an opportunity to prevent incumbent market participants' abuse of their dominant position. E.U. policymakers aim to avert the risk that a few large foreign firms would take control over an essential infrastructure to create barriers to entry.[230] As an alternative to the existing system of international negotiation under GATS that would require China to possibly change national telecommunications standards in favor of foreign market participants, it is instead seeking to export a centralized internet structure. Thus, China aims to create a possible parallel digital market based on Chinese-led standards and technology, based on a growing number of submarine cables being branched from Chinese territory.[231] These efforts to control information and data flows, internally and externally, have also been implemented via stringent limits imposed on foreign companies operating in the telecommunication sector.

Competition over the control of the infrastructure is also emerging in the context of new technology. Most notably, the implementation of 5G technology—the next generation of wireless mobile technology with greater data speeds, lower latency, and the possibility to connect more devices—is generating new friction. Chinese companies are the largest 5G developers globally, covering close to half of the global 5G networks.[232] The United States and many other partners have chosen to avoid such technology and develop new 5G networks.[233] The European Union's stance on this matter is not unequivocal, as some Member States view the adoption of Chinese technology favorably.[234]

Conflicts in the second layer emerge in the debates concerning the future of the internet. Traditionally, the Internet Corporation for Assigned Names

230. *Joint Statement on Electronic Commerce*, EUR. UNION (July 12, 2018), https://trade.ec.europa.eu/doclib/docs/2018/october/tradoc_157456.pdf (presenting an E.U. proposition to expand the Reference Paper with rules to enhance competitive safeguards in the monopolistic telecommunications market).

231. *See* Winseck, *supra* note 218.

232. *See* David Sacks, *China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond*, COUNCIL ON FOREIGN REL. (Mar. 29, 2021), https://www.cfr.org/blog/china-huawei-5g (outlining major external investment trends from China in 5G infrastructure worldwide).

233. Madison Cartwright, *Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle*, 9 INTERNET POL'Y REV. 1, 9-12 (2020) (arguing for the emergence of the "geo-economic spaces" based on division of different internet and technology companies).

234. *See* Sacks, *supra* note 232.

and Numbers (ICANN)—established in 1998 as a not-for-profit entity under California Law and subordinate to the U.S. Department of Commerce—standardized the IP and DNS governance system, setting the fundamental global standards critical to support the data routing systems of the internet. Following a proposal by the European Union and China to strengthen multilateral cooperation, the United States released control of ICANN to the international community in 2016, which internationalized the governance framework. [235] Currently, different positions at the U.N. International Telecommunication Union (ITU) are emerging. China, for example, has proposed a new standard for core network technology named New IP as part of broader efforts aimed at internationalizing its local decentralized internet infrastructure.[236]

The content layer is the third and most contentious layer. Companies exert significant market control through operating systems, search engines, and browsers.[237] Embracing liberal data governance, these companies have started collaborating with governmental agencies for various purposes, such as combatting terrorism, economic espionage, and international diplomacy.[238] As a reaction, the European Union and China alike have begun a process of decoupling by building their own higher layers.[239] In China, content is sealed off from the rest of the world by the Great Firewall—a system that turns the Chinese internet into an Intranet, restricting Chinese users from access to the World Wide Web, and keeping foreign users from penetrating the Chinese

235. Danielle Flonk, Markus Jachtenfuchs & Anke Obendiek, *Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?*, 9 GLOB. CONSTITUTIONALISM 364, 364-82 (2020) (presenting a dynamic of different viewpoints regarding the ultimate control of ICANN).

236. *See* Hoffmann et al., *supra* note 33.

237. Operating systems include iOS, Windows, and Android. The search engine market is dominated by Google. Facebook remains the biggest global social network, Amazon the largest global retailer, and ICANN is domiciled in the United States. For a deeper discussion, see Winseck, *supra* note 218.

238. *See* Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon & R.B.J. Walker, *After Snowden: Rethinking the Impact of Surveillance*, 8 INTL. POL. SOCIO. 121, 121-35 (2014) (discussing allegations of GAFAM firms handing information on users to intelligence services without their user's knowing).

239. For examples of movements away from GAFAM software, see Matt Hanson, *China to Ditch All Windows PCs by 2022—Could this Be Linux's Time to Shine?*, TECHRADAR, (Feb. 14, 2020), https://www.techradar.com/news/china-to-ditch-all-windows-pcs-by-2022-could-this-be-linuxs-time-to-shine; Wolf Richter, *LEAKED: German Government Warns Key Entities Not To Use Windows 8 Over Links To The NSA*, BUS. INSIDER, (Aug. 27, 2013), https://www.businessinsider.com/leaked-german-government-warns-key-entities-not-to-use-windows-8--links-the-nsa-2013-8.

intranet.[240] In the European Union, the upcoming Digital Services Act package is placing more responsibilities on digital service providers to incentivize the establishment of internal mechanisms of compliance, as regulated firms are expecting to cooperate with regulators in achieving stated principles.

As a result of these fundamental conflicts affecting each layer of the data infrastructure from emerging data governance regimes, fractures are increasingly inevitable, and consequences are poised to reshape the role of the internet at the center of data globalization. In particular, transnational data governance is developing along territorial lines, some of which are closed-loop, fragmenting, and potentially fracturing the commons of the internet.

IV. ADDRESSING THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE

The fragmented framework for transnational data governance generates a wicked problem. Characteristically, this type of problem features a conundrum, as any solution is only partial and bound to entail new issues. Fragmentation of the global framework for data governance, while increasing transaction costs and hampering the opportunities offered by cross-border data aggregation, undermines the core tenets of globalization. Yet, in a context of competing and conflicting regimes, any solution risks favoring one regime over the others, thereby exacerbating conflictual positions. Rather than one correct solution, this wicked problem can be addressed through different approaches targeting the most problematic aspects. In line with this view, addressing the wicked problem of transnational data governance entails harnessing the benefits of data globalization without undermining domestic sovereign priorities.

After having qualified fragmentation in transnational data governance as a wicked problem, this Section offers an analysis of the possible approaches that can be deployed to address it. The first approach is based on the global riparian system for water rights management. A riparian system for data flows would acknowledge the special status of data at the international level while mandating the coordination of bilateral mechanisms between jurisdictions. The second option consists of a plurilateral approach. In light of the

240. Laura Kirste & Dirk Holtbrügge, *Huawei at Bay? A View on Dependency Theory in the Information Age*, *in* HUAWEI GOES GLOBAL 291 (2020).

advantages brought by large networks of data, regulatory coalitions involving multiple jurisdictions could be established. Leveraging technology interoperability, regulatory coalitions could vary depending on regulatory matters and jurisdictions. The third option entails a multilateral approach. Under the aegis of proposals for a new DBW orDSB, international coordination could be established. We suggest that a combination of these approaches would provide a suitable solution, preventing further fragmentation. In particular, a DSB would offer a soft-law framework similar to those established to maintain financial stability, averting further ruptures in the global data flow, while offering a forum to mediate and resolve conflictual positions.

A. THE WICKED PROBLEM OF TRANSNATIONAL DATA GOVERNANCE

The fragmentation of the transnational governance framework generates a problem for which a clear and univocal solution is unattainable. Similar to climate change—whereby complex ecological chain reactions are intertwined with societal perceptions, political pressures, and economic incentives—transnational data governance requires untangling technological elements, domestic priorities, geopolitical tensions, and economic factors.[241] Any international solution to support a transnational framework for data governance, while entailing significant social benefits, would require overcoming critical hurdles.

International policy cooperation and coordination are essential to address common challenges. The establishment of internationally concerted rules on digital sovereignty, data securitization, and digital infrastructures would promote certainty on crucial matters, such as cross-jurisdictional data mobility and extraterritorial enforcement of domestic rules. Cybersecurity would also benefit from common standards. In a global economic landscape, trade,

241. *See* Gary E. Marchant, *Governance of Emerging Technologies as a Wicked Problem*, 73 VAND. L. REV. 1861, 1861-66 (2020) (noting that "the pace of technology development far outstrips the capability of regulatory systems to keep up"); Madeline Carr & Feja Lesniewska, *Internet of Things, Cybersecurity and Governing Wicked Problems: Learning from Climate Change Governance*, 34 INT'L REL. 391, 392-405 (2020) (comparing IoT and cybersecurity to climate change); Susan Ariel Aaronson, *Could Trade Agreements Help Address the Wicked Problem of Cross-Border Disinformation?*, CTR. FOR INT'L GOVERNANCE INNOVATION, (July 6, 2021), https://www.cigionline.org/publications/could-trade-agreements-help-address-the-wicked-problem-of-cross-border-disinformation/ (highlighting cross-border data as one of the sources of a transnational disinformation problem).

finance, and commerce would benefit from a safer environment if legal certainty and data integrity is ensured.[242] Even where jurisdictions prefer to maintain some level of control, domestic policies, international trade, and supply chains depend on data flows that move across jurisdictions. To achieve a minimum level of policy coordination, however, a common understanding is needed.

As the emerging data governance regimes have shown, the three major economies are solidifying intractable divergences in principal digital regulatory architecture. The U.S. approach encapsulates liberal market capitalism, which underpins the evolution of the internet but clashes with the consumer-centered and rights-based regime of the European Union, and with the increasingly controlled capitalism and state-centered structure deployed by China.

These considerations are not merely hypothetical. Internationally, two dynamics reflect the irreconcilable nature of domestic styles and the impossibility to reach a univocal solution.

First, unilateral approaches to the extraterritorial enforcement of rules alter the global data flows. This dynamic is particularly evident in the stances that the European Union has taken toward China and the United States. The GDPR establishes the principles of adequacy, whereby the transborder flow of personal data outside the Single Market can only occur if a certain level of protection is ensured.[243] In this context, E.U. officials have indicated that the expansive surveillance authority of China may never meet the criteria for adequacy recognition.[244] The E.U. rights-based regime has clashed with the American market-based regime: the CJEU has repeatedly deemed the U.S. data protection framework insufficient to ensure adequate protection of E.U. citizen data. In 2016, the CJEU ordered the shutdown of the Safe Harbor

242. On the risks of disruption in the commercial context, see *supra* Section II for a deeper discussion of the Chinese Cybersecurity Law.

243. *See* Streinz, *supra* note 64 and accompanying discussion in text.

244. Laurens Cerulus, *Europe Eyes Privacy Clampdown on China*, POLITICO, (Feb. 4, 2019) https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/.

Program[245] in the *Schrems I* judgment.[246] This stance was reiterated in 2020, when CJEU halted also the successor E.U.-U.S. Privacy Shield regime, which was a data-bridging mechanism allowing thousands of companies to self-certify for personal data transfer across the Atlantic in *Schrems II*.[247] At the core of the dispute was whether U.S. intelligence efforts concerning E.U. citizen data should remain out of the adequacy assessment, finding that they should remain within its scope.[248]

Second, jurisdictions are deploying competing strategies to extend their influence and control over data infrastructure. The California effect,[249] the Brussels effect,[250] and the Beijing effect[251] result in the diffusion of three competing models across the world's jurisdictions. Bilateral tensions are thus amplified, as they take a global stage. This dynamic is particularly evident in the context of the European Union. For instance, jurisdictions that aim to meet the GDPR adequacy standards must follow a specific procedure enshrined in Article 45. Accordingly, adequacy decisions are adopted by the European Commission, taking into account various elements, including general elements, such as "the rule of law, respect for human rights and fundamental freedoms,"[252] as well as specific aspects such as the existence of data protection laws, [253] the establishment of dedicated supervisory authorities,[254] and the commitment to third countries, international, regional or multilateral organizations for the protection of personal data.[255] In aligning with these criteria, jurisdictions seeking recognition for adequacy are required

245. *See* Churches & Zalnieriute, *supra* note 205 (outlining the consequences of the *Schrems* decision, including halting the EU-US Privacy Shield).

246. Case C-362/14, Maximiliam Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015). *See also*, Court of Justice of the European Union Press Release No. 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision is Invalid (Oct. 6, 2015).

247. Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020).

248. Theodore Christakis & Fabien Terpan, *EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options*, INT'L DATA PRIV. L. (2021). (highlighting the central nature of intelligence data access in E.U.-U.S. legal disputes and negotiations).

249. *See* HALEY & HALEY, *supra* note 142 and accompanying text.

250. *See* BRADFORD, *supra* note 23 and accompanying text.

251. *See* Erie & Streinz, *supra* note 31 and accompanying text.

252. GDPR, *supra* note 22, art. 45(2)(a).

253. GDPR, *supra* note 22, art. 45(2)(a).

254. GDPR, *supra* note 22, art. 45(2)(b).

255. GDPR, *supra* note 22, art. 45(2)(c).

to incorporate core aspects of the E.U. data governance regime, effectively expanding its influence but also reducing interoperability with U.S. and Chinese data governance.[256] To juxtapose, under the Beijing effect, jurisdictions are adopting the digital infrastructure of Chinese firms and adopting facets of its command-and-control variants of data sovereignty, which in turn are likely to reduce interoperability with E.U. and U.S. data governance.[257]

As divergent data governance regimes collide, ensuring both the security of data flows and legal certainty in the global data economy is difficult, if not impossible. While a single solution to the wicked problem of transnational data governance may not be possible, different approaches offer a variety of possibilities.

B. BILATERAL APPROACHES: THE RIPARIAN STATUS QUO

Water, like data, raises transnational concerns. 148 countries share at least one transboundary river basin and three-quarters of the world's nations house a river that crosses a political border.[258] Yet, there is no central agreement or international organization responsible for governing water rights. In fact, riparian approaches are naturally diverse, since they entail a wide variety of *sui generis* rules tailored to the needs of the parties involved to govern water rights, ownership, sovereignty, environmental matters, and public-private partnerships.[259] The U.N. Watercourse Convention—which has had a gestation period of 50 years and entered into force in 2014—aims to help

256. As of August 2021, the European Commission has recognized the following jurisdictions to provide adequate data protection: Andorra, Argentina, Canada (limited to commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom, and Uruguay. In June 2021, South Korea launched the procedure for recognition. *See Adequacy Decisions*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Jan. 5, 2023).

257. Erie & Streinz, *supra* note 31.

258. Rebecca L. Farnum, *Drops of Diplomacy: Questioning the Scale of Hydro-Diplomacy through Fog-Harvesting*, 562 J. HYDROLOGY 446, 447-86 (2018) (presenting a broad extent of stakeholders present in water-right related issues).

259. Joseph W. Dellapenna, *The Evolution of Riparianism in the United States*, 95 MARQ. L. REV. 53, 54-75 (2011) (highlighting the complexity and idiosyncratic development of water rights).

conserve and manage water resources. However, as of today, it has been ratified by only a few dozen jurisdictions.[260]

The current global riparian governance system is an apt analogy for the emerging fragmentation of transnational data governance. Like riparian governance, transnational data governance is increasingly based on domestic choices that, in turn, reflect distinctive governance styles and are embedded in competing and sometimes conflicting regimes. For instance, in the United States, access to water is not a federal matter; rather states implement different rules based on distinct doctrines for allocating rights.[261] Among various factors, the approaches adopted in each jurisdiction vary depending on availability, necessity, and sociopolitical considerations characterizing the local constituencies.[262] Hence, where water represents a scarce resource, a communitarian approach is favored; whereas, an abundance of water results in a more liberal market for water management.[263] The U.S. approach to data has followed a similar path, dominated by abundance and based on the protection of property rights to create a market for data. Alternatively, the European Union establishes standards for water quality and protection.[264] However, each country owns its own water bodies and jurisdictional issues are to be decided, with a unanimous voting mechanism, by the European Council,[265] the highest political body of the Union. The E.U. data governance regime presents an equivalent focus on privacy and data protection as fundamental rights. However, unlike in the case of water management, the European Union has

260. Convention on the Law of Non-Navigational Uses of International Watercourses, May 21, 1997, A/RES/51/229, https://digitallibrary.un.org/record/240629/.

261. Four general types of riparian doctrines have been observed. Absolute ownership allows water users to withdraw water from land without advance considerations to impacts of adjoining property. Reasonable use requires users to obtain a permit based on an evaluation of the reasonableness of the proposed beneficial use. Correlative rights grant water users rights in proportion to their land ownership or other allocation mechanisms. Prior appropriation water use rights are granted based on the timing of the appropriate to access water. *See* Dellapenna, *supra* 259.

262. The right to water is also a U.N. Sustainable Development Goal. On water as a right, see generally Sadia A. Jame & Laura C. Bowling, *Groundwater Doctrine and Water Withdrawals in the United States*, 34 WATER RES. MGMT. 4037 (2020).

263. *Id.*

264. Juliane Albrecht, *The Europeanization of Water Law by the Water Framework Directive: A Second Chance for Water Planning in Germany*, 30 LAND USE POL'Y 381, 381-95 (2013) (highlighting the complexities of water right regimes in the European Union).

265. DIRECTORATE-GENERAL FOR EXTERNAL POL'YS, EUR. PARLIAMENT, CONFLICT AND COOPERATION OVER WATER - THE ROLE OF THE EU IN ENSURING THE REALISATION OF HUMAN RIGHTS (2015).

been moving to establish a pan-E.U. system, where data is a common (and strategic) interest of the Union and its members. Finally, in China, the State owns the water and sets water rights via local governments and through water rights permits for local companies.[266] Similarly, data governance is now being centralized with State control and even ownership.

The parallel between data governance and the riparian system of water rights also explains transnational dynamics. First, global data flows have emerged as a part of a global network. Every user, public or private actor, connected to the internet is accessing digital data, and the broader pool of knowledge and information therein contained; similarly, people and entities connect to a shared body of water. Second, from a governance standpoint, competing and conflicting domestic interests restrain access to shared resources. In the same way alterations to a body of water upstream have consequences on communities living downstream, divergent data governance regimes implemented to reflect domestic idiosyncrasies have an impact on other jurisdictions and economies. As a result, international disputes arise but they are commonly resolved through bilateral mechanisms.[267]

Through this prism, a riparian approach to transnational data governance rests on two pillars. First, it suggests that, in the emerging fragmented framework, bilateralism is the most viable approach. Data governance, like water management, can remain anchored to a framework where different data-flow relationships are established on a case-by-case basis between different jurisdictions and actors. However, owing to the strategic importance of data, a second pillar is necessary to ensure that bilateralism does not deepen existing fractures. Like water, data can be awarded special status in international law. Even without a global framework for water management, jurisdictions have

266. David J. Devlaeminck & Xisheng Huang, *China and the Global Water Conventions in Light of Recent Developments: Time to Take a Second Look?*, 29 REV. EUR., COMPAR. & INT'L ENV'T L. 395, 395-410 (2020) (outlining the different approaches to water rights between China and other countries); Dajun Shen, Ali Guna & Xiaodan He, *Water Use Control System in China*, 36 INT'L J. WATER RES. DEV. 590, 590-601 (2020) (highlighting a state-centered water rights regime in China).

267. For example, there is an ongoing discussion about the diversion of water away from the Illi and Irtyish rivers between China and Kazakhstan. *See generally* Hongzhou Zhang & Li Mingjiang, *China and Global Water Governance*, *in* CHINA & TRANSBOUNDARY WATER POLS. ASIA (2017) (presenting an exhaustive discussion of water rights regimes and related discussions in Asia).

approached water as a vital resource that transcends policy compartments. In international discussions, water has been traditionally considered a commodity, but significant policy shifts have occurred in the past decade. In 2010, the United Nations passed a resolution explicitly recognizing access to water as a human right, that plays a crucial role in climate policy discussions.[268] In a similar vein, the special status of data, data flows, and data infrastructure could be recognized in international conventions to provide the basis for dispute adjudication and, possibly, minimum harmonization or a soft-law framework could be established to create standards to facilitate global cross-border data flow in different domains and, over time, establish a mechanism for the resolution of conflictual relationships.[269] Such approaches could be multilateral or plurilateral.

Conversely, a development trajectory following the riparian approach may also highlight the non-issue of the wicked problem. If fragmentation of data governance continues without cutting apart the growing data economy, fragmentation may just highlight the development of more niched, independent, and isolated sub-aspects of what, until now, has been a single mixed pot of state, market, and individual activities in cyberspace. The assertion of control over new data activity by jurisdictions via a riparian mixed-approach may thus be more indicative of rising complexities in data, rather than fragmentation.

C. PLURILATERAL APPROACHES: REGULATORY COALITIONS

A plurilateral approach could build on and expand the riparian approach to transnational data governance. Coalitions of jurisdictions based on sector-specific areas could be created with the intent of having uniform legal and regulatory treatment for sector-specific matters. This approach recognizes and legitimizes the existence of multiple data governance regimes. A jurisdiction may be part of different regulatory coalitions at the same time, depending on the types of data concerned, their use, and destination. For instance, data could

268. *See* Dellapenna, *supra* note 259; Emanuele Fantini, *An Introduction to the Human Right to Water: Law, Politics, and Beyond*, 7 WIRES WATER 1, 1-8 (2020) (arguing that in spite of United Nations recognition of the human right to water, it is a contested notion in regards to scope, content, and indicators).

269. *See generally* Bradley C. Karkkainen, *Multi-Jurisdictional Water Governance in Australia: Muddle or Model?*, *in* REFORMING WATER L. & GOVERNANCE: FROM STAGNATION TO INNOVATION IN AUSTRALIA 57 (Cameron Holley & Darren Sinclair eds., 2018) (presenting the challenges of managing shared basins of water).

follow different rules depending on the applicable regulatory coalition, as the same type of data can be used in trade, law enforcement, or knowledge contexts.

As current experience with adequacy standards has shown, regulatory coalitions entail the establishment of minimum standards. These standards can vary in degree of complexity, from broad adequacy regimes that would ascertain the fit of legal frameworks, like the GDPR, to much more nuanced systems of independent fiduciary data intermediaries that would grant permission for data flows to jurisdictions, private actors, and individuals alike depending on the type of data, their use, and related adequacy.[270] A prerequisite of this approach is that coalitions operate through a common set of technical rules within the same network.[271] In this scheme, a range of legal structures could provide the format of the intermediary.[272] Under the data trust model, legal trusts would be created to hold transferable data packages, in which fiduciaries manage what the data is used for and who has access to it for their client.[273] Trusts would hold data across jurisdictions, and offer a variety of risk appetites and management structures, allowing pre-authorized pools of data to be sent to appropriate third parties.[274]

Such a network could be used for both public and private actors. For example, jurisdictions could agree on networks of rules establishing how and what data can be transferred and through which channels. A variety of technologies are already available to help secure such messages, from DLT and blockchain applications to security-by-design solutions that can help guarantee

270. *See* Bruno Carballa Smichowski, *Alternative Data Governance Models: Moving Beyond One-Size-Fits-All Solutions*, 54 INTERECONOMICS 222, 222-30 (2019) (presenting different forms of fiduciary data trusts as a model for maintaining and sharing data).

271. *Id.*

272. *Id.*

273. Sylvie Delacroix & Neil D Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIV. L. 236, 236-47 (2019) (arguing that data trusts are key to enable different stakeholders to secure control over their data).

274. Other forms of data governance archetypes are closed, single source, data clearinghouse, data pool, and distributed. In a closed system, there is no sharing between data users and data holders. In a single source system, data holders receive data directly from data users. In a data clearinghouse system, there is an intermediary through which data holders can provide data to data users. In a data pool system, data holders pool data to an intermediary, which data users can access. The intermediary also reverts data to original data holders from the data users. In a distributed system, data holders and data users are intermingled. *See id.*

security of transmissions medium, to AI that can rapidly analyze the content of transmitted data. Private stakeholders could also create their own domain-specific networks. For instance, the SWIFT system of payments messaging could take part in this system. Data from local banks could be transmitted to a central standardized unit to automatically process and determine whether data is allowed to route through a given jurisdiction.[275]

Through regulatory coalitions, the issue of multiple internets is institutionalized with a technological solution that allows different interests and divergent regimes to coexist. Leveraging on existing networking technologies—that must be implemented in all jurisdictions—multiple sub-networks, with their own levels of permission, are branched together. This system would allow stability and security of the digital world,[276] without compromising the ability of individual entities and jurisdictions to determine levels of access.

Central to the plurilateral approach of regulatory coalitions is the existence of a shared network built to bolster the capacity to collect, store, process, and otherwise manipulate data. Within such a network, domestic idiosyncrasies are respected. Hence, regulatory coalitions can facilitate bilateral approaches to transnational data flows (based on a riparian approach), plurilateral regulatory systems, or offer the backbone for a truly multilateral approach, in the context of a new hard law DBW or a soft law DSB.

D. MULTILATERAL APPROACHES: A NEW (DIGITAL) BRETTON WOODS?

The lack of international fora to negotiate differences among regimes and calibrate rules offers a fertile ground for conflictual positions to escalate. In this context, the WTO—within the international framework set out by the GATS—represents the natural venue to define rights and obligations on data flows as well as core regulatory principles applicable to different types of data. To date, however, WTO members have not made specific commitments in this regard,[277] and the suitability of the WTO as an effective forum is in doubt. Outside the WTO, a new multilateral approach could be envisaged.

275. This system is similar to the Qualified Trust Service Providers established by the E.U. Second Payments Services Directive that certifies digital ID certificates by pinging back to domestic authorities.

276. DENARDIS, *supra* note 6.

277. Chu & Lee, *supra* note 129.

The divergent, competing and increasingly conflicting trajectories of data governance can aptly be compared to the international financial system in the first half of the twentieth century. Between the beginning of the First World War, in 1914, and the end of the Second World War, in 1945, the global financial system was fractured. Rampant currency devaluation leading to "beggar thy neighbor" policies, together with inconsistent cross-border trade rules and exclusionary trade blocs resulted in the breakdown of the transnational financial system and trade flows.[278] Following the end of the Second World War, in 1945, these problems led to the establishment of the Bretton Woods system, a multilateral framework to ensure monetary and financial stability. The Bretton Woods system was a hard law system, a treaty-based framework supporting cross-border interactions among fragmented financial and economic systems via the establishment of the International Monetary Fund (IMF) and the International Bank for Reconstruction and Development, which today is part of the World Bank Group. The aim was to promote global trade and to finance postwar reconstruction through fixed exchange rates and loans supporting economic recovery. As the global data economy is beset by similar instabilities in the context of post-pandemic recovery,[279] the model offers a possible blueprint to address the wicked problem of transnational data governance. Broadly, this idea has been framed as a new Bretton Woods—or a DBW—consisting of a general framework for transnational data governance based on a common set of rules.[280]

Such an overarching global framework would aim to offer a global paradigm for data governance, that is equipped to address the challenges of the Fourth Industrial Revolution. A DBW—like its analog-native predecessor—would stabilize the development of global infrastructures, and support the enactment of new legal rules and regulatory standards. Its role would dovetail with and support the shift from an industrial to a knowledge-

278. Thilo N. H. Albers, *Currency Devaluations and Beggar-My-Neighbour Penalties: Evidence from the 1930s*, 73 ECON. HIST. REV. 233, 233-41 (2020) (arguing that unilateral currency depreciations and trade blocks came at a high price to trade and finance).

279. *See generally* INTERNATIONAL MONETARY AND FINANCIAL LAW: THE GLOBAL CRISIS (Mario Giovanoli & Diego Devos eds., 2010) (presenting a broader discussion on the breakdown of the Bretton Woods monetary system and highlighting that its creation as well as breakdown was caused by crises).

280. *See* Medhara & Owen, *supra* note 38.

based global economy, where local and regional economic systems generate, collect, and protect information. Such a structure could be built on existing international initiatives. For instance, the recently formed E.U.-U.S. Trade and Technology Council—aiming to set high-level cooperation towards technology standards, supply chains, security, and competitiveness across the shores of the Atlantic—represents a stepping stone in this direction.[281] If its membership is extended, a global forum could be established. If its membership remains limited, it is likely to be the model for plurilateral approaches going forward.

As proposed, a DBW would achieve its objectives through three main functions.[282] Its primary function would be to provide a coordination mechanism, allowing the market-based United States, rights-based European Union, and state-centric China to hold a regulatory dialogue. Given the expanding tendency of the governance styles of these three jurisdictions, a coordination mechanism on key regulatory matters, such as competition, data mobility, and data securitization, would reverberate across the world regardless of whether jurisdictions decide to adhere to a given style or adopt a given regime, implement a local solution, or are still exploring different options. Beyond this key function, a DBW would also provide a forum where nascent challenges can be addressed. For instance, fundamental agreements on ethical principles concerning the use of data by algorithms and artificial intelligence is unlikely to be solved bilaterally (through a riparian system) or in a plurilateral manner (through regulatory coalitions). Second, the DBW would oversee negotiations over data-related agreements. Based on a set of core principles governing the interoperability of data flows for essential services— such as finance, law enforcement, and public health—a DBW could assist discussions on various international initiatives, including the current debates over the establishment of a global tax regime for digital services.[283] Third, a DBW could perform a legal and regulatory harmonization function.

281. Press Release, Eur. Comm'n., EU-US Launch Trade and Technology Council (June 15, 2021), https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

282. *See* Medhara & Owen, *supra* note 38.

283. This framework would expand and take ownership of existing initiatives like the OECD/G20 Inclusive Framework on Domestic Tax Base Erosion and Profit Shifting. For a general discussion, see generally Veronika Solilová, Danuše Nerudová & Marian Dobranschi, *Profit Shifting and Tax Base Erosion in the Twenty-First Century*, *in* PROFIT SHIFTING & TAX BASE EROSION 9 (2021) (providing background to the inclusive framework on profit shifting and tax base erosion).

The DBW would also entail core organizations. As the digital divide is hindering development and growth, the hiatus between centers and peripheries must be addressed through dedicated programs of technical assistance and capacity building, supporting jurisdictions to develop and leverage their digital infrastructures through knowledge transfers. These new roles can be performed in coordination with existing multilateral organizations, such as the World Bank and the IMF. A novel, treaty-based framework, however, is hard to be implemented and, as history has shown, critical challenges have ultimately led to enacting a decentralized global financial system.[284] In this context, a global framework for transnational data governance can be established as a soft-law system.

In particular, a soft-law institution can be established as a functional twin institution to the Financial Stability Board,[285] focused on the stability of global data flows.[286] Such an entity, the DSB, may be part of the DBW or operate as a soft-law entity initiated by the G20, as is the case for the Financial Stability Board. It would have three main responsibilities. First, it would represent the engine to promote legal and regulatory harmonization, coordinating the development of policies, principles, and standards across the most salient areas of data governance.[287] Against a shared core of rules and principles, jurisdictional and regional adjustments and variations could be implemented to reflect different priorities and needs.[288] Second, the DSB would perform a monitoring role, assessing the vulnerabilities arising from the use of data-based

284. Though the Bretton Woods monetary system provides a model for an umbrella policing of transnational governance, the system also proved to have significant limits and was displaced by decentralized global financial markets. *See generally* INTERNATIONAL MONETARY AND FINANCIAL LAW, *supra* note 279, at 8-35 (presenting a broader discussion on the breakdown of the Bretton Woods monetary system, highlighting that its creation as well as breakdown was caused by crises—typical of most changes in international financial law regimes).

285. The Financial Stability Board was set up to find common regulatory ground among the global banking and insurance industry and cover regulatory gaps after the global financial crisis.

286. Robert Fay, *Digital Platforms Require a Global Governance Framework*, CTR. FOR INT'L GOVERNANCE INNOVATION (Oct. 28, 2019), https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/.

287. *Id.*

288. Typically, domestic approaches may diverge on the treatment of social media content and competition policies.

technologies to recommend possible course of actions.[289] This activity may be performed in cooperation with the ITU, the Institute of Electrical and Electronics Engineers, ICANN, and other organizations.[290] Finally, the DSB would provide a critical information hub, providing aggregate information and statistics on data governance and flows. For instance, more accurate data would be available to domestic authorities regarding the data treatment of large platforms—such as GAFAM and BATs. In a similar vein, organizations like the WTO and the IMF could benefit from the information gathered by DSB to modernize their rules and policies to better meet the needs of the data economy.

While a DBW would offer a suitable framework to address the wicked transnational data governance problem, its implementation presents some difficulties. In particular, an international consensus must be reached to establish such a system. Its operability would ultimately depend on the level of cooperation, with a G20 centered soft law DSB much more likely to be possible at least initially than a full multilateral agreement.

V. A PATH FORWARD?

In this Article, we have considered the wicked problem of transnational data governance. This wicked problem stems from the interaction of increasingly different, competing and conflicting data governance regimes fragmenting the global framework that underpins transnational data flows and the global data economy. Left unaddressed, the wicked problem risks regressing transnational cooperation in any area that benefits from unrestrained data flows. This is a significant risk in the face of both the benefits that global digital commons entail and the dangers posed by digital threats to the international community. These risks have been dramatically increased as a result of the invasion of Ukraine.

Our contribution is threefold. First, we provide a systematic identification of challenges arising from the emerging fragmentation of transnational data governance and data globalization. Second, we develop a comprehensive

289. *See* Fay, *supra* note 286.

290. A DSB could also help unite a variety of private organizations that have risen in recent years to address pressing challenges, such as the International Grand Committee Against Disinformation, which unites experts sharing recognition of online platforms, or the Global Partnership on AI.

analytical framework to understand the emergence of governance styles and the ensuing materialization of conflicting regimes in the United States, the European Union, and China. This, in turn, allows us to assess the depth of the impact that a fragmented framework for transnational governance has on global data flows. Third, we show the wicked nature of such a problem, for which there is no definitive solution. Instead, we offer three lanes of approaches—entailing bilateralism, plurilateralism, and multilateralism—that could be adopted by the international community to facilitate cross-border data flow, while minimizing clashes with domestic interests.

Moving from our investigation, a series of actionable conclusions can be drawn. First, a balanced combination of the three approaches appears to be a more palatable way to address the transnational data governance problem than their discrete application; in fact, it is a necessity. In consideration of the ongoing competition, offering the ability for jurisdictions to choose—and most importantly, switch—between data governance styles is essential to de-escalate tensions, promote sectoral cooperation, and pave the way for mending fractures in the global flows of data. Moreover, in the current geopolitical context, bilateralism is the most practical and likely starting point, with plurilateralism gradually evolving along with a truly multilateral system. As data becomes a key priority for trade and other transnational policies, plurilateral approaches are a natural evolution to leverage the benefit of larger networks. Sectoral coalitions are likely to increase support for global finance and international trade. Yet only a multilateral approach allows ensuring a minimum level of coordination, even respecting domestic idiosyncratic preferences. At the very least, it would create a single point of reference for handling conflicts in international data flows. While which combination of the three approaches will emerge is yet to be seen, current trends indicate the reinforcement of plurilateral and multilateral approaches.

Through this prism, the second crucial point that our investigation reveals is the necessity to steer away from an uncoordinated bilateral system. Plurilateral approaches to transnational data governance allow data actors such as states, businesses, or individuals to draw on the benefits of the economies of scale. Especially in the digital economy, the availability and frictionless access to data—even without ownership or exclusive control—is becoming increasingly important. Relatively frictionless data travel or access is a necessity

to ensure the efficient functioning of a number of critical networks. For example, SWIFT depends on the ability of banks to receive and send messages across several entities before payment is confirmed. Hence, sectoral coalitions—with adequacy requirements similar to those implemented in the European Union through the GDPR—may leverage existing initiatives where data circulates freely among participating jurisdictions for specific purposes. Current trends in global finance envisage the establishment of data-exchange systems between banks and law enforcement agencies to combat money laundering activities. Similarly, as an increasingly large pool of stakeholders need to be connected to a single network to verify data on trade, goods, services, and parties, major emerging platforms that support supply-chain finance would benefit from regulatory coalitions. Regulatory coalitions might also be the only solution for economies or sectors where data is not available, or access is limited. Connecting to a larger network becomes essential for developing AI applications.

Following this trajectory, plurilateral data governance coalitions are likely to shape the majority of transnational data governance relationships. As public and private actors are likely to seek access to several coalitions at once, multiple adequacy requirements must be met, and their compliance needs to be ensured across different networks. The ability of jurisdictions to switch among a variety of fragmented and disconnected transnational frameworks provides a strong incentive to establish a formal body that both oversees the integrity of the shared network and facilitates the negotiation of any contentious matters. A DSB could perform this role.

Finally, and more broadly, a third conclusion can be drawn highlighting the importance of a DSB that represents a vital component of any solution. The development of legal, regulatory, and technical standards can support bilateral arrangements for data flow, plurilateral networks, and multilateral systems. A DSB, at the most basic level, can identify best practices and minimum requirements in a variety of fields, from cybersecurity and ethical use of AI to protocols for data transfer. At a more advanced level, it may act as a neutral clearing channel (at least) for critical data.

The result is a balanced transnational governance framework that does not require a complete de-fragmentation of the transnational data governance, nor does it require a treaty-based DBW. Instead, it empowers jurisdictions to choose their data governance relationships by providing a standardized

method for opening, closing, and swapping between data channels and regimes. Flexibility and data circulation are, thus, ensured, even in the case of multiple internets, given that this system could manage an increasing amount of connecting and disconnecting transnational data networks.