THE BEIJING EFFECT: CHINA'S "DIGITAL SILK ROAD" AS TRANSNATIONAL DATA GOVERNANCE*

Matthew S. Erie† and Thomas Streinz‡

New York University Journal of International Law and Politics (forthcoming).

DRAFT. Please check for and cite the published version once available.

ABSTRACT

China shapes transnational data governance by supplying digital infrastructure to emerging markets. The prevailing explanation for this phenomenon is "digital authoritarianism" by which China exports not only its technology but also its values and governance system to host states. Contrary to the one-size-fits-all digital authoritarianism thesis, this Article theorizes a "Beijing Effect," a combination of "push" and "pull" factors that explains China's growing influence in data governance beyond its borders. Governments in emerging economies demand Chinese-built digital infrastructures and emulate China's approach to data governance in pursuit of "data sovereignty" and digital development. China's "Digital Silk Road," a massive effort to build the physical components of digital infrastructure (e.g., fiber-optic cables, antennas, and data centers), to enhance the interoperability of digital ecosystems in such developing states materializes the Beijing Effect. Its main drivers are Chinese technology companies that increasingly provide telecommunication and e-commerce services across the globe. The Beijing Effect contrasts with the "Brussels Effect" whereby companies' global operations gravitate towards the EU's regulations. It also deviates from US efforts to shape global data governance through instruments of international economic law. Based on a study of normative documents and empirical fieldwork conducted in a key host state over a four-year period, we explain how the Beijing Effect works in practice and assess its impact on developing countries. We argue that "data sovereignty" is illusory as the Chinese party-state retains varying degrees of control over Chinese enterprises that supply digital infrastructure and urge development of legal infrastructures commensurate with digital development strategies.

---

* This Article has benefitted from presentations given at Harvard Law School, the Hertie School of Governance, the U.S.-Asia Law Institute at New York University School of Law, and Yale Law School. The authors thank José Alvarez, Anu Bradford, Prasenjit Duara, Rebecca Hamilton, Benedict Kingsbury, Aynne Kokas, Elisa Oreglia, Shitong Qiao, and Katharin Tai for their comments on earlier drafts. All errors are the authors'.

† Associate Professor of Modern Chinese Studies, Oriental Institute and Associate Research Fellow, Centre for Socio-Legal Studies, University of Oxford. Email: matthew.erie@orinst.ox.ac.uk. This Article is part of the "China, Law and Development" project (https://cld.web.ox.ac.uk), funded by the European Research Council (Grant No. 803763)

‡ Adjunct Professor of Law and Executive Director of Guarini Global Law & Tech at New York University School of Law. Email: thomas.streinz@law.nyu.edu. This Article draws on insights from the Global Data Law project at Guarini Global Law & Tech (www.guariniglobal.org/global-data-law) and projects at the Institute of International Law and Justice (IILJ) on Infrastructures as Regulation (www.iilj.org/InfraReg/) and Megaregulation and International Legal Ordering (www.iilj.org/MegaReg).

TABLE OF CONTENTS

I. Introduction

The People's Republic of China's (PRC's or China's) emerging role in global governance in the twenty-first century has become increasingly prominent with the PRC's sprawling Belt and Road Initiative (BRI) assuming center stage as a new model for global economic ordering.[1] The BRI encompasses a wide array of infrastructure projects to enhance the movement of goods, labor, capital, and energy between China and countries ranging from Vanuatu to Venezuela, creating connections through land, sea, and even space. Such infrastructure projects potentially have significant local and regional impacts and may, in the aggregate, facilitate China-dependent value chains. As part of this process, firms rely crucially on information and telecommunication technology to operate decentralized or "unbundled" production networks transnationally.[2] For this and other purposes, China has, alongside its traditional infrastructure projects, been building digital complements packaged as the "Digital Silk Road" (*shuzi sichou zhilu*) to supply connectivity in terms of international communication and data flows.[3] This digital infrastructure complements the land-based Silk Road Economic Belt and the Twenty-First Century Maritime Silk Road, which supply connectivity by providing enhanced transport capacity for physical goods.

This Article asks whether and to what extent the "Digital Silk Road" (DSR) influences data governance outside China. The conventional account is that China exports its "model" of technological control in what analysts have termed "digital authoritarianism."[4] We find this explanation insufficient for a number of reasons, including its assumption that there exists a "China model" and that this template can be unproblematically transplanted to other jurisdictions.[5] Instead, our response to this question is what we term the "Beijing Effect": a combination of "push" and "pull" factors

---

[1] *See* NADÈGE ROLLAND, CHINA'S VISION FOR A NEW WORLD ORDER (National Bureau of Asian Research Special Report No. 83) (2020) (arguing that China seeks partial hegemony over the "global South"); Julien Chaisse & Mitsuo Matsushita, *China's 'Belt and Road' Initiative: Mapping the World Trade Normative and Strategic Implications*, 52 J. WORLD TRADE 163, 167 (2018) (finding that China seeks a "radically new approach towards international trade and investment"); Julien Chaisse, *Introduction: China's International Investment Law and Policy Regime - Identifying the Three Tracks*, *in* CHINA'S INTERNATIONAL INVESTMENT STRATEGY: BILATERAL, REGIONAL, AND GLOBAL LAW AND POLICY 1, 12 (Julien Chaisse ed. 2018) (concluding that China will be a rule-maker in the long term); BRUNO MAÇÃES, BELT AND ROAD: A CHINESE WORLD ORDER (2018) (arguing China presents an alternative value system than Western globalization); *but see* Gregory Shaffer & Henry Gao, *A New Chinese Economic Order?* 23 J. INT'L ECON. LAW 607 (2020) (arguing that China's model repurposes Western law and institutions); Matthew S. Erie, *Chinese Law and Development*, HARV. INT'L L. J. (forthcoming) (drawing attention to China's approach to law and development and the salience of extralegal and nonlegal norms alongside instruments of international economic and commercial law); Jiangyu Wang, *China's Governance Approach to the Belt and Road Initiative (BRI): Partnership, Relations, and Law*, 14 GLOBAL TRADE & CUSTOMS J. 222 (2019) (identifying China's approach to global trade and investment as flexible, pragmatic, and result-oriented); Prasenjit Duara, *The Chinese World Order in Historical Perspective: The Imperialism of Nation-States or Soft Power*, 2 CHINA AND THE WORLD: ANCIENT AND MODERN SILK ROAD 1 (2019).

[2] RICHARD BALDWIN, THE GREAT CONVERGENCE: INFORMATION TECHNOLOGY AND THE NEW GLOBALIZATION (2016).

[3] *See infra* text accompanying notes 171 – 175.

[4] *See infra* text accompanying notes 40 – 42.

[5] *See infra* text accompanying notes 44 – 46.

that explains China's growing influence in "transnational data governance."[6] By *transnational data governance*, we mean the rules, norms, practices, and infrastructures governing the collection, storage, transfer, use of, and access to digitalized information (i.e., data) across national borders.[7] As an extension of its discourse on global Internet governance, in which China has consistently advocated for "cyber sovereignty," China has come to emphasize "data sovereignty" for its internal data governance regime, thereby asserting the legitimacy of governmental control over data flows.[8] Unlike the EU and the U.S., China has not leveraged legal instruments to directly influence other countries' data governance regimes. Yet, through the DSR, Chinese companies are increasingly supplying the digital infrastructure that forms an integral part of any data governance regime. Developing countries that exhibit growing demand for such infrastructures, may find the prospect of "data sovereignty" particularly appealing.

We argue, however, that "data sovereignty" is illusory for most developing countries as the power to govern data effectively is dependent on controlling all relevant digital infrastructure, much of which is increasingly being supplied by Chinese technology companies, which are, in turn, operating – to varying degrees – under the influence of the Chinese Communist Party (CCP). Consequently, while certain BRI states may be drawn towards data governance environments that are more or less "closed" (in the sense of allowing for a certain degree of governmental control over both in-country and cross-border data flows), they remain ultimately "open" to intervention and pressure from the PRC. The extent to which governments can counterbalance continued and growing Chinese influence in the digital domain is not just a function of their relative power and financial and infrastructural dependence on China, but also dependent on the strength of their domestic legal and political systems.[9] The question, then, is how or whether smaller states can draw the line between their own rule and one shaped by China.

The DSR and its impact on data governance outside China are intertwined with the global expansion strategies of China's massive electronic commerce and information and telecommunications (ICT) technology companies. Alibaba has positioned itself as a global e-commerce platform for small and medium-sized enterprises (SMEs) and is internationalizing this strategy through the electronic world trade platform (eWTP).[10] Companies such as Huawei and ZTE are providing networking equipment that is fundamental for broadband Internet and "Internet of Things" applications in "smart" and "safe" cities. TenCent's Weixin (WeChat), a social media platform, and ByteDance's TikTok, a video-sharing app, facilitate communication between billions across the globe. In recent years, these companies' entry into the markets of the U.S., U.K., Europe, and Japan has incited broad debate, mostly revolving around privacy and national security

---

[6] *See also* Sheena Chestnut Greitens, *Dealing with Demand for China's Global Surveillance Exports*, BROOKINGS (Apr. 2020), https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/ (identifying "push" and "pull" factors for demand for Chinese surveillance technology).

[7] *See infra* text accompanying footnotes 28–39.

[8] *See infra* text accompanying footnotes 118–124 and 330–337.

[9] *See infra* text accompanying footnotes 338–345.

[10] *See infra* text accompanying footnotes 204–207.

concerns, but also touching on questions of technological and economic hegemony.[11] Whereas significant attention has been paid to these companies' presence in the markets of Western states in both the academic and popular literature, to date, there is little analysis of their impact on developing countries, where very different dynamics are emerging in regards to China's presence in the digital landscape.[12]

Under the BRI, China is supplying infrastructure and capital not only to some mature markets in Europe but primarily to emerging economies. The BRI involves, in addition to traditional infrastructure projects like highways, railroads, and power plants, the DSR, components of *digital infrastructure*, that is, infrastructure for the transfer, storage, and processing of data.[13] These digital infrastructures are assemblages of physical elements (e.g., fiber-optic cables, antennas, and data centers) and non-physical counterparts (e.g., transmission standards, networking protocols, and digital identifiers). Given that digital infrastructure in developing countries is often embryonic, the impact of Chinese firms' activities in these markets might be more consequential than their presence in Western post-industrial societies, especially those with strict investment review regimes in the tech sector.[14]

Theorizing the Beijing Effect captures how China influences data governance transnationally, and, in particular, the extent to which Chinese companies are shaping the digital infrastructure in a developing country under the DSR. Our assessment of the DSR is based on careful analysis of normative documents in Chinese and English, including laws, regulations, industry reports, and cases, supplemented by Chinese media analyses, mainly to track developments among Chinese companies. We also draw on think tank research,[15] committee reports,[16] and the emerging scholarship on the DSR from various

---

[11] Karl P. Sauvant, *Is the United States ready for FDI From China? Overview*, *in* INVESTING IN THE UNITED STATES: IS THE US READY FOR FDI FROM CHINA? (Karl P. Sauvant ed. 2009); JI LI, THE CLASH OF CAPITALISMS? CHINESE COMPANIES IN THE UNITED STATES (2018); Jeffrey N. Gordon & Curtis J. Milhaupt, *China as a "National Strategic Buyer": Toward a Multilateral Regime for Cross-Border M&A*, 1 COLUM. BUS. L. REV. 192 (2019).

[12] There are, of course, exceptions. *See, e.g.*, Chan Jia Hao & Deepakshi Rawat (2019). *China's Digital Silk Road: The Integration of Myanmar* (RSIS Commentaries, No. 084). RSIS COMMENTARIES, https://hdl.handle.net/10356/84321; Joshua Eisenman & Eric Heginbotham, CHINA STEPS OUT: BEIJING'S MAJOR POWER ENGAGEMENT WITH THE DEVELOPING WORLD (2018).

[13] *See* Martin Hilbert and Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE 60 (2011) (describing the dominance of digital technologies for telecommunication and information storage and processing).

[14] In the wake of the coronavirus pandemic, there has been an increasing divergence in views on Chinese investment between developed and developing countries with the latter much more open to continuing business with Chinese. *See* BRUNSWICK. UNDERSTANDING GLOBAL OPINION OF CHINESE BUSINESSES: A GROWING DIVIDE BETWEEN DEVELOPED AND EMERGING MARKETS (2020) (on file with the authors) (finding, among the general population of 23 countries where Chinese invest, that 80% of respondents from emerging economies trusted Chinese companies, an increase of 3 percentage points from 2018 whereas only 51% of respondents from developed economies, a decrease of 5 percentage points from 2018, trusted Chinese companies).

[15] Cave et al., *Mapping China's Technology Giants*, AUSTRALIAN STRATEGIC POLICY INSTITUTE: REPORT NO. 15 (2019); Sen Gong et al., *The Impact of the Belt and Road Initiative Investment in Digital Connectivity and Information and Communication Technologies on Achieving the SDGs*, K4D EMERGING ISSUES REPORT (2019); Robert Greene & Paul Triolo, *Will China Control the Global Internet Via its Digital Silk Road?,* SUPCHINA (May 8, 2020), https://carnegieendowment.org/publications/81857; Joshua

disciplines.[17] We further complemented our theoretical work with empirical research, carried out through in-country interviews in Pakistan, a key country in China's DSR, between 2017 and 2020, in what is perhaps the first instance of fieldwork on the local impact of the DSR in a BRI partner state. This integration of theoretical and empirical work strikes us as important because the BRI, including the DSR, remains notoriously difficult to study due to the inaccessibility of core materials (especially, normative documents such as memoranda of understanding which outline inter-state commitments). Such sources are mostly not publicly disclosed for a variety of reasons ranging from commercial secrecy to national security. Our fieldwork provides empirical insights on developments on the ground to make the BRI, often characterized by lofty aspirations, more accessible and analyzable.

In this Article, we hope to connect and engage strands of literature across various inter- and intradisciplinary fields of scholarship. Our focus on transnational data governance brings together a range of issues conventionally discussed by legal scholars under varying, but also overlapping, rubrics of cyberlaw, data protection and privacy law, information law, and telecommunications law, including from comparative perspectives. It also necessitates an interdisciplinary approach that integrates the important work by scholars of communications and Internet studies.[18] By highlighting the salience of *infrastructure*, we echo findings made by Internet governance scholars[19] and respond to the call to integrate insights from the interdisciplinary field of infrastructure studies into legal analysis.[20] Our case study of DSR's impact on Pakistan seeks to respond to long-standing questions about the relationship of *law and development* with the innovation that the PRC – and not the traditional "developed countries" [21] – is driving the development

---

Kurlantzick, *Assessing China's Digital Silk Road: A Transformative Approach to Technology Financing or a Danger to Freedoms?*, COUNCIL ON FOREIGN RELATIONS (Dec. 18, 2020), https://www.cfr.org/blog/assessing-chinas-digital-silk-road-transformative-approach-technology-financing-or-danger.

[16] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2019 REPORT TO CONGRESS 266-68 (discussing the DSR); U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2018 REPORT TO CONGRESS (devoting a whole chapter to China's high-tech development and "next generation connectivity").

[17] *See* Hong Shen, *Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative*, 12 INTL. J. OF COMM. 2683 (2018).

[18] *See* Rohinton P. Medhora et al., *Data Governance in the Digital Age*, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION SPECIAL REPORT (2018).

[19] Laura DeNardis and Francesca Musiani, *Governance by Infrastructure, in* THE TURN TO INFRASTRUCTURE IN INTERNET GOVERNANCE 3–21 (Francesca Musiani et al., eds., 2014); MILTON MUELLER, WILL THE INTERNET FRAGMENT? (2017); DAVID D. CLARK, DESIGNING AN INTERNET (2018).

[20] Benedict Kingsbury, *Infrastructure and InfraReg: on rousing the international law 'Wizards of Is'*, 8 CAMBRIDGE INT'L. L. J. 171 (2019).

[21] David M. Trubek & Marc Galanter, *Scholars in Self-Estrangement: Some Reflections on the Crisis in Law and Development Studies in the United States*, 4 WIS. L. REV. 1062 (1974); JAMES A. GARDNER, LEGAL IMPERIALISM: AMERICAN LAWYERS AND FOREIGN AID IN LATIN AMERICA (1980); Brian Tamanaha, *The Lessons of Law-and-Development Studies*, 89 AM. J. INT'L. L. 470 (1995); Michael Trebilcock & Jing Leng, *The Role of Formal Contract Law and Enforcement in Economic Development*, 92 VA. L. REV. 1517 (2006); DAVID M. TRUBEK & ALVARO SANTOS, THE NEW LAW AND ECONOMIC DEVELOPMENT (2006); David M. Trubek, *Law and Development: Forty Years after 'Scholars in Self-Estrangement'*, 66 UNIV. OF TORONTO L. J. 301 (2016).

agenda.[22] Finally, our Article is fundamentally concerned with the rise of China as a global power, a topic with great importance that draws commensurate interest from a wide range of disciplines, including international law and global governance, international politics and international relations, and China studies.[23]

The commitment to intra- and interdisciplinarity also animates our ongoing large-scale research projects from which this Article draws. The "China, Law and Development" project studies the role of law in the PRC's global development.[24] This Article shares that ambition and sheds light on the ways in which the DSR, as part of the BRI, affects data governance in host states, thereby emphasizing the salience of domestic legal instruments to effectively regulate the economic, social, and cultural implications of digital infrastructures. This insight connects with a certain strand of the "InfraReg project," which recognizes the regulatory effects of infrastructures – commonplace in urban studies and science and technology studies (STS) but under-examined in the legal scholarship – and asks whether and how law regulates such infrastructures.[25]

As this Article shows, BRI states' international and domestic Internet policies are deeply intertwined with physical infrastructures such as terrestrial and underwater fiber-optic cables, Internet Exchange Points, and the antennas necessary for broadband cellular networks. Moreover, the "Internet of Things" technologies that are being deployed in "smart" and "safe" cities have transformative potential for the lives and livelihoods of citizens.[26] The common denominator of all these technologies is data. Access to and use of data is fundamentally regulated by digital infrastructures but is increasingly also an object of legal regulation and an instrument of ordering on various scales – notions that the "Global Data Law" project sets out to explore.[27] What we find in the context of the PRC's development of the DSR is the absence of transnational legal ordering in the digital domain compared to approaches pursued by the EU and the U.S. and, rather, the presence of infrastructural ordering as the construction, maintenance, and operation of digital infrastructures by Chinese companies, which transforms the conditions under which emerging economies transition into a digital future.

The remainder of this Article is organized as follows: Part II analyzes China's impact on data governance transnationally. Contrary to "digital authoritarianism," we develop our account of the "Beijing Effect," and then show how China influences data governance beyond its borders. China's domestic data governance regime employs

---

[22] China has been more active in Africa, as promoting innovation in industrial policy, including technology, than in other regions. *See generally*, CHRIS ALDEN ET AL., CHINA RETURNS TO AFRICA: A RISING POWER AND A CONTINENT EMBRACE (2008); DEBORAH BRÄUTIGAM, THE DRAGON'S GIFT: THE REAL STORY OF CHINA IN AFRICA (2009).

[23] ANDRE GUNDER FRANK, REORIENTING THE 19TH CENTURY: GLOBAL ECONOMY IN THE CONTINUING ASIAN AGE (2015) (resituating world history with Asia, and specifically China, at the center of the global economy); AMERICA, CHINA, AND THE STRUGGLE FOR WORLD ORDER (John Ikenberry, Wang Jisi, and Zhu Feng, eds., 2015); KISHORE MAHBUBANI, HAS CHINA WON? THE CHINESE CHALLENGE TO AMERICAN PRIMACY (2020) (viewing U.S. stagnation in the face of China's dynamism).

[24] *See also* Matthew S. Erie, *supra* note 1.

[25] More information about the project is available at www.iilj.org/infrareg.

[26] *See infra* §IV.B.

[27] More information about the project is available at www.guariniglobal.org/global-data-law.

territorial data localization requirements in pursuit of "data sovereignty." Developing countries are drawn to the promise of governmental control over data flows and the ostensible economic success of China's development of its digital economy. This effect is amplified by China's advocacy for "data sovereignty" in various global data governance institutions and reinforced by Chinese companies increasingly providing digital infrastructures in developing countries and influencing technical standard-setting for emerging digital technologies. In Part III, we show how the Beijing Effect materializes in the context of the DSR. In lieu of a comprehensive legalized structure, the DSR relies on several non-binding bilateral and multilateral instruments for international coordination between China and DSR host states that spell out the relationship between connectivity, sovereignty, and established international institutions. Part IV zooms in on Pakistan as a case study to examine how China influences data governance in a host state under the DSR. The DSR provides digital connectivity in the China-Pakistan Economic Corridor (CPEC) and Chinese technology companies are engaged in various "safe" city projects in Pakistan. At the same time, Pakistan's legal infrastructure for data governance lacks adequate safeguards and mirrors China's in prioritizing national security over citizens' data privacy. Part V evaluates the Beijing Effect in the context of the DSR's impact on digital development in host states. "Data sovereignty" is untenable for most developing countries and building digital infrastructures without developing appropriate legal infrastructures is unlikely to be sustainable. Part VI concludes.

II. China's Transnational Impact on Data Governance

Before explaining how the PRC increasingly shapes data governance transnationally through the Beijing Effect, we clarify our terminology. We use the terms "data governance," "transnational," and "infrastructural" in distinctive ways that may depart from their usage elsewhere. By *data governance* we mean the rules, norms, practices, and infrastructures governing the collection, storage, transfer, use of, and access to digitalized information (i.e., data).[28] This data-centered concept is broader than narrower conceptions that would only focus on certain kinds of information and only on their regulation through law. By encompassing all data, the conception of data governance used in this paper includes categories of data that are conventionally subject to certain specialized legal rules – as well as all data for which no such rules exist. For example, data governance encompasses personal data as protected by data protection and privacy laws; certain information with intellectual property protections; the textual, visual, or audio information protected by freedom of expression under international human rights law and domestic constitutional law. But data governance also addresses data for which no such specialized rules exist (e.g., non-personal, factual data collected

[28] This definition departs from the use of "data governance" and "data management" in company settings. *See* Vijay Khatri & Carol V Brown, *Designing Data Governance*, COMMUNICATIONS OF THE ACM (2010), https://doi.org/10.1145/1629175.1629210 (distinguishing between data governance as encompassing IT-related decision domains and accountability mechanisms and data management as making and implementing of decisions).

by a sensor about the weather in a certain locality).[29] By venturing beyond formal law, our conception of data governance includes societal or cultural norms about the handling of data as well as institutional practices. We also recognize the immense practical importance of (legally non-binding) technical standards. These standards may be issued by formal standard-setting organizations, consortia of technology companies, or even by a single developer.[30] Such data-related standards may address the handling of data (such as ISO's 27001 standard for information security),[31] but also define formats in which data is being stored (such as Adobe's PDF format), maintain protocols for data transmissions (such as the Internet's foundational TCP/IP protocol), or create design-specifications to ensure interoperability (such as the fourth generation LTE standard for wireless telecommunication).

Our use of *transnational data governance* extends beyond the idea of the regulation of cross-border data flows. Our account includes the various ways in which one domestic data governance regime may have effects on others as well as the use of international law or other international norms and standards to shape data governance across borders. Domestic data laws may have intended or unintended spillover effects, such as those caused by territorial data localization requirements.[32] Certain data laws lend themselves to explicit or implicit extraterritorial application.[33] Additionally, some domestic data laws rely on the unilateral or bilateral assessment of the "adequacy" of another country's data law to regulate data transnationally.[34] All these "legal technologies" of transnational data governance are best understood as attempts to exercise effective jurisdictional control over data. International law, either in the form of dedicated data protection or cybersecurity treaties and increasingly by way of commitments under international economic law, may also shape the ways in which different jurisdictions regulate data.[35] However, the extent to which data is increasingly governed transnationally by legal means, whether rooted in domestic or international law, is layered onto and intertwined with transnational data governance instruments that are not legally binding but may have no less (or even more) regulatory effect. This is especially true for technical standards, but may also apply to certain guidelines and principles that are widely observed in practice. Ultimately, the regulatory effect of any data governance framework can only be established by scrutinizing its implementation in practice.

---

[29] *But see* Nadezhda Purtova, *The Law of Everything*, 10 LAW, INNOV. AND TECH. 40 (2018) (arguing that the distinction between personal and non-personal data should be abandoned and *all* data processing should be governed by legal rules).
[30] *See* C. Bradford Biddle, *No Standard for Standards: Understanding the ICT Standards Development Ecosystem*, in THE CAMBRIDGE HANDBOOK OF TECHNICAL STANDARDIZATION LAW: COMPETITION, ANTITRUST, AND PATENTS 17 (J.L. Contreras ed. 2017).
[31] *See* Eric Lachaud, *ISO/IEC 27701: Threats and Opportunities for GDPR Certification*, Working Paper (discussing the relationship between relevant ISO standards and GDPR certification schemes).
[32] *See infra* text accompany notes 104–116.
[33] *See infra* text accompany notes 96–104.
[34] *See infra* text accompany notes 58–59 and 119.
[35] *See infra* text accompany notes 125–135.

Finally, we distinguish between *legal* and *infrastructural* data governance. This echoes to some extent the insight that Lawrence Lessig popularized with the catch-phrase "code is law" in the 1990s,[36] but our use here is broader, attuned to the digital landscape in the twenty-first century, and arguably, more multi-layered than Lessig's original postulate. Lessig's theory identified architecture as a form of regulation separate from but comparable to regulation by social norms, market mechanisms, and law. He posited that "cyberspace"[37] was, to a significant extent, governed by its own architecture (i.e., "code") which he defined as the hardware and software that make cyberspace what it is and thereby regulates it.[38] Consequently, the code-makers become important regulators themselves and governmental regulation through formal law might need to target code itself to achieve the desired regulatory outcome. While Lessig's basic insight still holds, it requires updating. Technologically, Lessig wrote when the Internet became commercialized and the World Wide Web took off. Today, the Internet has penetrated societies and economies everywhere – persistent digital divides notwithstanding – and has transcended its initial communication functions to become the fundamental infrastructure for other digital technologies unimaginable without it. In Laura DeNardis's analysis: the Internet is in everything, and this has implications for both its regulation and regulatory effects.[39] Politically, Lessig's normative framework was the U.S. Constitution. This framing cannot accommodate a multipolar landscape in which digital technologies, with global reach, are being developed and deployed transnationally by foreign (from the U.S. perspective) corporations and governments. Put differently, it cannot account for the Beijing Effect.

A. The Beijing Effect

In this section, we develop a theoretical account to explain how China is increasingly influencing data governance beyond its borders. The conventional explanation for understanding how China influences technological development beyond its borders is "digital authoritarianism." This view holds that just as China has evolved an approach to technology that enhances its control over society, sidelines opponents and dissent, disseminates propaganda and disinformation, and fosters economic exchange without liberal human rights, so too is China transplanting such technology-based

---

[36] *See* Lawrence Lessig, CODE: AND OTHER LAWS OF CYBERSPACE (1999). Lessig was not the first legal scholar to recognize the regulatory effects of "code." *See* Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEXAS L. REV. 552 (1998). The insight that physical objects can have regulatory effects (and associated "politics") is usually ascribed to social scientist Langdon Winner, *Do Artifacts Have Politics?*, 109 DAEDALUS 1 (Winter 1980).

[37] The usefulness of the "cyberspace" moniker has been contested for decades: *contrast* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (conceptualizing cyberspace as a separate locality for purposes of legal analysis) and Richard Ford, *Against Cyberspace, in* THE PLACE OF LAW 147 (Austin Sarat et al., eds., 2003) (rejecting a metaphysic of space in Internet law discourse). We avoid the term as it is not central to our analysis.

[38] *See* Lawrence Lessig, CODE VERSION 2.0 (2005), at 5. The original theory was developed in Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

[39] Laura DeNardis, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH (2020).

enablers of repressive rule across borders.[40] Specifically, governments and corporations rely on surveillance, censorship, social manipulation, cyber attacks, Internet enclosures, and targeted persecution to effect such goals.[41] The digital authoritarianism thesis has become popular among think tanks that promote democratic values globally.[42] It has also become a mainstay in the academic literature on China, particularly in the vein of the "China model."[43]

While we do not disagree with many of the findings of the "digital authoritarianism" literature, we find that there are three problematic assumptions underlying this argument. First, the thesis assumes a "China model." There is no consensus in the literature as to what the China model is, and definitions vary from boilerplate autocracy to meritocratic experimentation.[44] For a China model to exist (let alone be replicable), a certain form of government (e.g., one-party state) and strategies of state-building (e.g., infrastructure urbanization and demographic engineering) would be necessary but not sufficient; it would also require a specific historical formation of the relationship between the party-state and society (i.e., late-comer modernization and exposure to Western imperialism that effected a civil war that, in turn, set the stage for a dominant political party that, following a decade of violence, ushered in a period of globalization). In short, the Chinese party-state (not to mention the Chinese economy and population) is idiosyncratic. The second and related assumption is that nondemocratic states are interchangeable. The idea is that autocracies, kleptocracies, quasi-military regimes, "illiberal democracies," and hybrid regimes (e.g., anoncracies) all operate through the same rules. This assumption is not borne out, as demonstrated by the case of

---

[40] *See e.g.*, Valentine Weber, *Understanding the Global Ramifications of China's Information-Control Model*, *in* ARTIFICIAL INTELLIGENCE, CHINA, RUSSIA, AND THE GLOBAL ORDER 76 (Nicholas D. Wright, ed. 2019); Alina Polyakova and Chris Meserole, *Exporting Digital Authoritarianism: The Russian and Chinese Models*, BROOKINGS INSTITUTE POLICY BRIEF (2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Naazneen Barma, Brent Durbin, and Andrea Kenall-Taylor, *Digital Authoritarianism: Finding Our Way Out Of The Darkness*, WAR ON THE ROCKS (Feb. 10, 2020), https://warontherocks.com/2020/02/digital-authoritarianism-finding-our-way-out-of-the-darkness/.

[41] Steven Feldtein, *When It Comes to Digital Authoritarianism, China Is A Challenge – But Not The Only Challenge*, WAR ON THE ROCKS (Feb. 12, 2020), https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/.

[42] *See e.g.*, Adrian Shabaz, *The Rise of Digital Authoritarianism*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (last visited Nov. 24, 2020); Erol Yayboke, *Promote and Build: A Strategic Approach to Digital Authoritarianism*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES BRIEFS (Oct. 15, 2020), https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

[43] *See e.g.*, Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, *The Digital Dictators: How Technology Strengthens Autocracy*, 99 FOR. AFFAIRS 103, 104 (2020) (describing "digital autocracies"); Willem Gravett, *Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa*, 20 AFR. HUM. RIGHTS L. J. 125, 125 (2020) (finding that "the 'China model' of digital governance is a palatable guise for a far-reaching system of state censorship …")

[44] *See generally* RANDALL PEERENBOOM, CHINA MODERNIZES: THREAT TO THE WEST OR MODEL FOR THE REST? (2007); Zhu Yunhan (朱云汉), Wen Tiejun (温铁军), Zhang Jing (张静)& Pan Wei (潘维), *Gongheguo Liushi Nian yu Zhongguo Moshi* (共和国六十年与中国模式) [*People's Republic at 60 Years and the China Model*], 9 DUSHU (读书) [READING] 16 (2009); DANIEL A. BELL, THE CHINA MODEL: POLITICAL MERITOCRACY AND THE LIMITS OF DEMOCRACY (2015).

Pakistan.[45] The third assumption regards the mechanics of borrowing. Digital authoritarianism assumes the export of Chinese governance in a way that is both unilateral and positions China as the dominant party. Again, the case of Pakistan disproves a facile cut-and-paste process.[46]

Drawing on the literature of regulatory competition, we develop an alternative account, which we shorthand as the "Beijing Effect." This term is inspired by Anu Bradford's "Brussels Effect", which is the prevailing theory for understanding how law may have regulatory effects outside its jurisdiction of origin.[47] The PRC's approach to data governance and its effect on third countries, however, is not explainable by the kind of unilateral global regulation that Anu Bradford has theorized for the EU. While imposing costs on foreign companies required to comply with its data localization requirements, the PRC's domestic data governance regime does not exhibit the features that would give rise to a "Beijing effect" of the kind that Bradford describes.

There are, however, other mechanisms through which China exerts influence on foreign data governance regimes. China's approach to domestic data governance and its concept of "data sovereignty" appeal to certain governments which emulate it within their domestic systems, even without explicit PRC pressure to do so. Moreover, there is considerable demand for digital infrastructures which Chinese companies increasingly provide globally, thereby inextricably inserting themselves into domestic data governance regimes abroad. These two dynamics coincide with China's assertive promoting of "data sovereignty" in Internet governance institutions and the increasing influence of Chinese companies in technical standard-setting. The "Beijing Effect" captures these developments, explains their drivers, and may be helpful in developing counter strategies.[48]

The Beijing Effect is best explained in contrast to the Brussels Effect as theorized by Bradford. The Brussels Effect posits that companies gravitate towards European law even when they are not legally required to do so. As Bradford explains, this is a dynamic comparable to the "California effect" that David Vogel has analyzed in the U.S. regulatory systems where companies adjust to California's environmental regulations resulting in a "race to the top."[49] Bradford's key insight is that these dynamics also play out globally with the EU assuming the role of global regulator in a variety of regulatory domains. The preconditions for this effect to occur are: market power, regulatory capacity, relatively high standards, inelasticity of the relevant consumer market, and companies' preference for uniformity.[50]

---

[45] *See infra* §IV.
[46] DANIEL MARKEY, CHINA'S WESTERN HORIZON: BEIJING AND THE NEW GEOPOLITICS OF EURASIA 4-6 (2020).
[47] ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020); the book expands her argument as initially developed in Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).
[48] *See infra* §V.
[49] DAVID VOGEL, TRADING UP: CONSUMER AND ENVIRONMENTAL REGULATION IN A GLOBAL ECONOMY (1995).
[50] *See* Bradford, THE BRUSSELS EFFECT (2020) *supra* note 47, at 25–66.

The EU's data protection regime is often presented as a key example of the Brussels Effect.[51] The EU's General Data Protection Regulation (GDPR) asserts jurisdiction over the processing of European personal data, regardless of where such processing takes place.[52] Firms cannot simply evade the reach of European data protection law by way of data de-localization and might hence opt for compliance with European data protection law anywhere.[53] The GDPR imposes high cost for non-compliance by threatening sanctions of up to 4% of global turnover for GDPR violations.[54] Since global tech corporations need to comply with the GDPR, they may choose to follow its rules everywhere. Even though Facebook initially responded to the GDPR's entry into force by moving (non-European) user data out of the GDPR's jurisdictional reach,[55] it came to endorse the GDPR as a global standard and ended up offering GDPR-compliant settings to its users everywhere (though not by default).[56]

Bradford's thesis has influenced the emergent field of transnational data regulation. Paul Schwartz has argued that Bradford's account of unilateral regulatory globalization overplays the unilateral power of the EU to dictate the terms of global data protection regulation.[57] The GDPR limitations on the cross-border transfer of personal data have led to complex negotiations to acquire the coveted "adequacy" status which allows for exports of personal data from the EU to third countries.[58] Japan secured the first (pro forma) bilateral rather than unilateral recognition of adequacy with the EU, while the EU and U.S. have been engaged in a protracted back and forth about the adequacy of U.S. data protection laws.[59] Schwartz posits that countries might emulate the European data protection regime not primarily because of firms lobbying for global

---

[51] *See* Bradford, THE BRUSSELS EFFECT (2020) *supra* note 47, at 131–147; Cedric Ryngaert and Mistale Taylor, *The GDPR as* Global *Data Protection Regulation?*, 114 AJIL UNBOUND 5 (2020).

[52] *See* Regulation (EU) 2016/679, of the European Parliament and the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (hereinafter GDPR), art. 3. The GDPR applies to data processing regardless of location, if carried out by a data controller who is established within the EU. The GDPR also applies to data processing by a data controller not established in the EU, if related to offering goods or services or monitoring the behavior of data subjects who are in the EU. These jurisdictional features give the GDPR global reach.

[53] *See* Thomas Streinz, *Data Governance in International Economic Law: Non-Territoriality of Data and Multi-nationality of Corporations* (manuscript, on file with author) (discussing the interplay between strategic incorporation and data governance).

[54] GDPR, art 82.

[55] Alex Hern, *Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law*, THE GUARDIAN (Apr. 19, 2018), https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.

[56] Heather Kelly, *Facebook Will Push Privacy Alert to Users Outside EU Ahead of GDPR*, CNN BUSINESS (May 24, 2018), https://money.cnn.com/2018/05/24/technology/facebook-gdpr-us/index.html.

[57] Paul Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019).

[58] GDPR, articles 44, 45.

[59] Paul Schwartz, *supra* note 57 at 786–793; *See also* HENRY FARRELL AND ABRAHAM L. NEWMAN, OF PRIVACY AND POWER: THE TRANSATLANTIC STRUGGLE OVER FREEDOM AND SECURITY (2019). The EU Court of Justice struck down the EU-US "safe harbor" arrangement in Case C-362/14, Maximillian Schrems v Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015). The successor "privacy shield" suffered the same fate in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020).

uniformity but because of a growing global consensus on data protection. This consensus manifests itself in international instruments such as the Council of Europe's Data Protection Convention and a wide array of non-binding but still influential global data protection instruments which recognize the EU's approach as appealing because of its comprehensive nature (in contrast to the U.S.'s sectoral approach). While not refuting Bradford's account, Schwartz complicates it in useful ways by pointing to different dynamics of "push" and "pull" and by foregrounding a wider array of mechanisms of influence, most notably international agreements.

We build on Bradford's and Schwartz's work by exploring China's influence on global data governance in the context of the DSR. Bradford concludes that China does not yet exert the kind of regulatory influence that the EU has demonstrated or, in other words, a "Beijing Effect" (in her usage) is unlikely in the near term.[60] We agree that China is not likely to bring about a "Beijing Effect," as Bradford conceives of it. While China certainly has the market size to attract companies from around the world,[61] market size alone is insufficient to induce global compliance with domestic law. The quality of regulations is a key factor. In this regard, the standard critique of Chinese law is that it suffers from poor implementation despite being proficient "on the books."[62] It remains to be seen whether China's regulatory capacity specifically for data governance suffers from the kind of inadequate enforcement that has hamstrung Chinese law in the past. China's data governance regime is still nascent. While it aspires to a high level of comprehensiveness and sophistication—its Cybersecurity Law and accompanying measures are in many respects more advanced than analogous U.S. legislation—there remain a number of ambiguities about the regime and how it will be enforced.[63]

The key reason why China is unlikely to replicate the Brussels Effect is that foreign digital economy companies do not favor a globalization of the Chinese approach to data governance. Companies may prefer uniformity in global data governance in principle, but this depends on the commensurability of divergent regimes and their respective costs. While there is significant overlap between the EU's GDPR and China's

---

[60] *See* Bradford, *The Brussels Effect* (2012), *supra* note 47 at 49 (proposing "It will be a while before China could replace the EU as a source of de facto global standards") and Bradford, THE BRUSSELS EFFECT (2020) *supra* note 47 at 266 (arguing the unlikeliness of a "Beijing Effect" along the lines of her Brussels Effect). *See also* Alan Beattie, *Technology: How the US, EU and China Compete to Set Industry Standards*, FINANCIAL TIMES (July 24, 2019), https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271.

[61] By World Bank metrics, China is nearly tied with the EU as the second largest economy in the world, as measured by GDP, after the US. *See GDP (current US$) – European Union, United States, China*, THE WORLD BANK, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=EU-US-CN (last viewed Aug. 17, 2020).

[62] Donald C. Clarke, *Puzzling Observations in Chinese Law: When is a Riddle Just a Mistake? in* UNDERSTANDING CHINA'S LEGAL SYSTEM: ESSAYS IN HONOR OF JEROME A. COHEN 93 (C. Stephen Hsu ed. 2003); RANDALL PEERENBOOM, CHINA'S LONG MARCH TOWARD RULE OF LAW 323 (2002). *See also* Bradford 2020, 31 (citing China's "lack of effective and independent bureaucratic institutions overseeing national market rules in this area").

[63] *See* Huang *infra* note 92 (noting that China's data governance regime suffers from uneven enforcement); see further discussion of China's data governance framework *infra* text accompanying notes 82–108.

emerging data governance framework,[64] differences persist that make it unfeasible or undesirable for global corporations to have a uniform company-wide standard. Global technology companies may prefer a fragmented landscape under which they serve customers according to the respective domestic law instead of amplifying costly domestic data governance frameworks globally. Data is, to a certain extent, an elastic regulatory target (not unlike financial capital) and business preference for global uniformity of data governance has limits. A fragmented regime is neither technologically impossible nor necessarily prohibitively costly. In contrast to divergent manufacturing standards that often incur considerable switching costs, multi-national companies may change the ways in which they store and process data relatively rapidly and in cost-effective ways. This might also become the fate of the Brussels Effect: if the costs imposed by the EU's data protection regime exceed the benefit of global uniformity, companies will fragment their products for different markets. While this is not (yet) a reality for the EU, it is the prevailing corporate strategy regarding China's data governance regime.[65]

While China does not demonstrate Bradford's version of the Beijing Effect, we suggest that there is already a Beijing Effect of a different kind, and one that is likely to grow. We theorize three mechanisms, each a combination of "push" and "pull" dynamics, through which China affects transnational data governance: First, foreign government emulate China's approach to data governance and its promise of "data sovereignty," aided by China's promotion of that concept in global Internet governance institutions and other venues. Second, Chinese actors play increasingly important roles in digital technology standard-setting. [66] Fueled by the "Made in China 2025" plan, which seeks to ensure the country's self-reliance in high-tech sectors, Chinese companies, particularly Huawei, lead the development of the global 5G standard.[67] China's assertiveness in digital technology standards builds on its use of its own technical and industrial standards in its physical infrastructure projects overseas.[68] Digital technology standards traverse across borders through adoption in international standard-setting organization or if multinational companies gravitate towards a common standard to ensure interoperability.[69] It is particularly in this regard, that foreign companies maintain an interest in cooperating with China. They may not gravitate towards Chinese law – as the

---

[64] *See* Bradford, THE BRUSSELS EFFECT (2020) *supra* note 47, at 153 (arguing that the Cybersecurity Law emulates the GDPR "at least on its face").
[65] *See infra* text accompany notes 115–116.
[66] Shin-yi Peng, *Standard as a Means to Technological Leadership? China's ICT Standards in the Context of the International Economic Order*, *in* CHINA IN THE INTERNATIONAL ECONOMIC ORDER (Lisa Toohey, et al., eds., 2015); U.S.-China Business Council, *China in International Standards Setting: Recommendations for Constructive Participation* (2020), https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf.
[67] *See* Paul Triolo and Allison Sherlock, *'New Infrastructure' — China's Race for 5G and Networked Everything Has a New Catchphrase*, SUPCHINA (Jul. 1, 2020), https://supchina.com/2020/07/01/new-infrastructure-chinas-race-for-5g-and-networked-everything-has-a-new-catchphrase/. *But see* Diester Ernst, *Competing in Artificial Intelligence Chips: China's Challenge amid Technology War*. CIGI REPORT (Mar. 26, 2020), https://www.cigionline.org/publications/competing-artificial-intelligence-chips-chinas-challenge-amid-technology-war (discussing China's reliance on foreign semiconductors).
[68] Olivier Peyrat, *Normes: Un outil cache de la stratégie économique chinoise*, 6 LE JOURNAL DE L'ÉCOLE DE PARIS DU MANAGEMENT 30 (2012).
[69] *See* C. Bradford Biddle, *supra* note 30 at 17 (explaining the genesis of ICT standards).

Brussels Effects postulates for EU law – but towards common technical standards to maintain interoperability with Chinese technology. Third, Chinese companies provide digital infrastructures and platforms in host countries along the DSR, thereby shaping the conditions under which these countries transition towards digitally mediated economies and societies. Emerging economies show growing demand for digital infrastructure provided by Chinese technology companies — a process that may paradoxically undermine the host state's ambitions towards "data sovereignty."[70] So while certain push dynamics are discernible, it is in the force of the pull whereby the Beijing Effect is most consequential.

In sum, Beijing is not Brussels. China's data governance regime does not exhibit the characteristics that have been instrumental in turning the EU's GDPR into a "*Global* Data Protection Regulation," but a "Beijing Effect" with different characteristics is plausible. The result is not a replication of the PRC's domestic data governance laws as a "China model," or in comparative law terms, "legal transplants," but an endorsement of its underlying data governance principle of governmental and territorial control over data that materializes in different and highly context-dependent domestic data laws.[71] Chinese technology companies may, depending on the relative sophistication of local law, take advantage of host state legal systems granting them particular market access and operational liberties. Of course, Chinese technology companies are not unique in their penetration of emerging markets and supplying of digital infrastructure;[72] however, their entanglement with the Chinese party-state distinguishes the China case and makes the Beijing Effect unique.[73] In the following section, we explain the three mechanisms of the Beijing Effect in more detail, beginning with China's approach to data governance, and compare and contrast China's influence on data governance transnationally with the roles that the EU and U.S. play.

B. China's Approach to Data Governance: Data Localization in Pursuit of Data Sovereignty

China has borrowed from other jurisdictions and innovated its own approach to data governance. The notion of "cyber sovereignty" (*wangluo zhuquan*), the idea to assert national jurisdiction over the Internet in China, is central to its data governance regime and shapes how Chinese citizens engage with the outside world and vice versa.[74] The PRC's data governance framework is driven by the twin objectives of protecting national security (first and foremost) while also fostering economic growth. Even General

---

[70] *See* discussion of this claim *infra* §V.
[71] *See infra* §IV.C. for discussion of Pakistan's domestic data governance framework under (indirect) Chinese influence.
[72] For instance, Hewlett Packard has provided surveillance technology to monitor Uyghurs. *See* Liza Lin and Josh Chin, *U.S. Tech Companies Prop Up China's Vast Surveillance Network*, WALL ST. J. (Nov. 26, 2019), https://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846?mod=rsswn.
[73] *See infra* IV.C.
[74] *See* Rogier Creemers, "China's Conception of Cyber Sovereignty: Rhetoric and Realization" (on file with the authors) (citing the Information Office of the State Council's *White Paper on the Internet in China* (2010)).

Secretary of the CCP and PRC President Xi Jinping is promoting what the World Economic Forum calls the "fourth industrial revolution": the fusion of the digital, biological, and physical worlds.[75] The PRC government, along with China's technology giants, has transformed social governance in the country with recourse to digital technologies, in particular big data analytics and artificial intelligence/machine learning applications.[76] Innovations that are now commonplace in China include a cashless society,[77] a social credit system,[78] a "health code" that monitors citizens for infectious diseases,[79] and online courts to handle disputes.[80] Despite—or because of—this coordinated effort to shape digitalization in accordance with Beijing's priorities of social stability, China has the largest e-commerce market, the highest number of Internet users, and the fastest growing technology companies in the world.[81]

We do not offer a full account of China's burgeoning data governance framework in this Article.[82] Instead, we focus on the elements that are salient for its transnational

---

[75] Xi Jinping, Rang meihao yuanjing bian wei xianshi: zai jin zhuan guojia ren yuehanneisibao huiwu da (让美好愿景变为现实—在金砖国家领导人约翰内斯堡会晤大范围会议上的讲话) [Making a Beautiful Vision a Reality: Speech at the Grand Meeting of the Leaders of the BRICS Countries in Johannesburg], (Jul. 26, 2018), http://www.qstheory.cn/zhuanqu/2018-07/27/c_1123186013.htm (speaking of the technological revolution of big data, artificial intelligence, and other cutting-edge technologies). The "Made in China 2025" plan is part of this goal. The "fourth industrial revolution" moniker was coined by WEF founder Klaus Schwab.

[76] Zhongguo xinxi tongxin yanjiuyuan Anquan yanjiusuo (中国信息通信研究院安全研究所) [China Academy of Information and Communications Technology, Security Research Bureau] Dashuju anquan baipishu (大数据安全白皮书) [Big Data Security White Paper] 1 (2018) (calling big data a "core strategic resource and a key factor in society's basic production").

[77] Rui Zhong, *China Can't Afford a Cashless Society*, FOREIGN POL'Y (Sept. 11, 2018), https://foreignpolicy.com/2018/09/11/china-cant-afford-a-cashless-society/ (discussing problems accompanying digital payments in China).

[78] Assessments vary considerably. *See, e.g.*, Yu-Jie Chen, Ching-Fu Lin, and Han-Wei Liu, *"Rule of Trust": The Power and Perils of China's Social Credit Megaproject*, 32 COLUM. J. ASIAN L. 1 (2018–2020); Liav Orgad & Wessel Reijers, *How to Make the Perfect Citizen? Lessons from China's Model of Social Credit System*, EUROPEAN UNIVERSITY INSTITUTE WORKING PAPERS RSCAS 2020/28 (describing China's model of "cybernetic citizenship" and how it parallels and diverges from Western systems); Rogier Creemers, *China's Social Credit System: An Evolving Practice of Control* (May 9, 2018), available at SSRN: https://ssrn.com/abstract=3175792. Xin Dai, *Towards a Reputation State: A Comprehensive View of China's Social Credit System Project*, *in* SOCIAL CREDIT RATING (Oliver Everling, ed.) 139 (2020).

[79] "Geren jiankang xinxi ma" xilie guojia biaozhun jiedu (《个人健康信息码》系列国家标准解读) [Interpretation of the Series of National Standards Pertaining to the "Personal Health Information Code"], Zhejiang biaozhun xinxi pingtai (浙江标准信息平台) [Zhejiang Standards Information Platform] (May 22, 2020), http://www.zjsis.com/contents/2000/496143.html.

[80] Jason Tashea, *China's All-Virtual Specialty Internet Courts Look Set to Expand into Other Areas of the Law*, ABA JOURNAL (Nov. 1, 2019), https://www.abajournal.com/magazine/article/china-all-virtual-specialty-internet-courts.

[81] Jeff Desjardins, *China's Home-Grown Tech Giants Are Dominating Their US Competitors*, BUS. INSIDER (Feb. 7, 2018), https://www.businessinsider.com/chinas-home-grown-tech-giants-are-dominating-their-us-competitors-2018-2?r=UK (showing how Baidu, Alibaba, Tencent, and Xiaomi have outpaced Google, Apple, Facebook, and Amazon in terms of international market penetration).

[82] There is a growing comparative law literature examining the different approaches to data governance in the U.S., EU, and China. *See, e.g.*, Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PA. ST. J. OF L. & INT'L AFF. 50 (2020); Jeanne Huang,

effects. We show how China exercises jurisdictional control over data by mandating territorial data localization of certain categories of data. This exhibits similarities but also important differences with the EU's approach under the GDPR, which entails elements of extraterritorial application and subjects foreign jurisdiction to a unilateral "adequacy assessment." Recently, the U.S. has also shown an interest in targeted data localization aimed at Chinese technology companies.[83] But China's regime, including its approach to territorial data localization, remains distinctive.

China's data governance regime is constantly evolving and features a number of overlapping domains including telecommunication regulation, online content management, cross-border data flows, encryption, and critical infrastructure security.[84] The rules that govern these overlapping areas are not purely legal; in addition to legislation and regulatory measures, non-legally binding standards (not to be confused with technical standards) and strategies also play important roles with varying ambit.[85] For example, the "Thirteenth Five-Year Informatization Plan" (2016), sets out a number of objectives for the "informatization" of all aspects of society.[86] Along these lines, an array of legislation, measures, and standards provide increasingly specific guidance on how data should be managed to achieve the PRC's strategic aims.

There are multiple governmental agencies responsible for promulgating these different types of normative documents. The main agencies are the Ministry of Public Security (MPS), which is charged with maintaining Internet safety, the Ministry of Industry and Information Technology (MIIT), the central regulator of the Internet, and the Cyberspace Administration of China (CAC), which was established in 2011 with the mandate of overseeing online content regulation, and has increasingly centripetal authority.[87] Below this trinity, at the national level, there are a number of additional agencies with some oversight over data governance issues, including the National Development and Reform Commission, Ministry of Finance, People's Bank of China, and the Ministry of Science and Technology, among others. China's major technology

---

Applicable Law to Transnational Personal Data: Trends and Dynamics, 21 GERMAN L. J. 1283 (2020); Henry S. Gao, *Data Regulation with Chinese Characteristics* (draft on file with the authors).

[83] Since fall 2019, the Committee on Foreign Investment in the United States (CFIUS) has been reviewing Bytedance's acquisition of Musical.ly in November 2017, which was later merged into TikTok; the question, whether TikTok is transmitting data about US users to China is reportedly a key focus of the inquiry; *see* Robert McMillan et al., *TikTok User Data: What Does the App Collect and Why Are U.S. Authorities Concerned?*, WALL ST. J. (Jul. 7, 2020), https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084; *see also* Misty Hong v. Bytedance, Inc., 2019 WL 6481689 (N.D.Cal.) (Trial Pleading) (alleging that "TikTok clandestinely has vacuumed up and transferred to servers in China vast quantities of private and personally-identifiable user data that can be employed to identify, profile and track the location and activities of users in the United States now and in the future").

[84] Samm Sacks, *China's Emerging Cyber Governance System*, CENTER FOR STRATEGIC & INT'L STUDIES, https://www.csis.org/chinas-emerging-cyber-governance-system (last visited May 28, 2020); *see also* Gao *supra* note 82.

[85] *See* Sacks *supra* note 84.

[86] State Council, "'Shisanwu' guojia xinxihua guifan de tongzhi ("十三五"国家信息化规范的通知) [Notice on the Thirteenth Five-Year Informatization Plan], promulgated Dec. 27, 2016, http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm.

[87] *See* Gao *supra* note 82.

companies and a growing number of think tanks also seek to shape China's data governance policies. Provincial-level bodies (governmental, corporate, academic) may promote their own interests that do not always mirror those of national-level authorities. Hence, there are a number of voices and industry needs that determine how different kinds of data should be stored, processed, used, and transferred.[88]

The key legislation in China's data governance regime is the Cybersecurity Law (2017).[89] Central to the Cybersecurity Law is its treatment of what it calls "personal information" and "important data." "Personal information" pertains roughly to what the GDPR terms "personal data" or information that is related to an identified or identifiable natural person.[90] "Important data" is broadly defined as data that is closely related to national security, economic security, or social stability.[91] There is a robust black market for data in China that traffics in data through identify theft, hijacking, fraud, and other data-based crimes.[92] China's approach to data governance targets unlawful use of personal information by non-state actors but lacks adequate barriers to governmental intrusion of privacy.[93] In May 2020, the Third Session of the Thirteenth National People's Congress (NPC), the main legislative organ in the Chinese system, passed a Civil Code, the first of the PRC, which further specifies that personal information is protected by law.[94] The NPC Standing Committee work report, which details which

---

[88] Samm Sacks, Paul Triolo, and Graham Webster, *Beyond the Worst-Case Assumptions on China's Cybersecurity Law*, NEW AMERICA, https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/ (last visited Aug. 17, 2020).

[89] Zhonghua renmin gongheguo wangluo anquanfa (中华人民共和国网络安全法) [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 (hereinafter, "Cybersecurity Law").

[90] GDPR, art. 4(1).

[91] "Shuju anquan guanli banfa (zhengqiu yijiangao)" gongkai zhenqiu yijian de tongzhi (《数据安全管理办法（征求意见稿）》公开征求意见的通知) [Public Notice for Seeking Comments on the "Measures on Data Security Management" (Draft for Seeking Comment)], issued by the State Internet Information Office on June 28, 2019, Art 38(5), http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm.

[92] Huang Shujing [黄姝静], Shuju heishi changjue, yinsi pin zao xielou, ruhe lifa du shang geren xinxi loudong (数据黑市猖獗，隐私频遭泄露，如何立法堵上个人信息漏洞) [The Black Market is Rampant, and Privacy is Frequently Leaked. How to Legislate to Plug Personal Information Loopholes?] CAIJING ZAZHI (财经杂志) [CAIJING MAGAZINE], May 29, 2020, http://finance.ifeng.com/c/7wsCSAIVDeq (providing one example whereby, during the height of the coronavirus outbreak in Wuhan, the persona data of 7,000 residents of Wuhan city was leaked through social media apps).

[93] *See e.g.*, Cybersecurity Law, art 12 (distinguishing the state as "protecting the rights of citizens, legal persons, and other organizations to use networks in accordance with the law" from "[a]ny person and organization [who] using networks shall abide by the Constitution and laws."). *See also* Zuigao renmin fayuan, zuigao renmin jiachayuan (最高人民法院，最高人民检察) [Supreme People's Court, Supreme People's Procuratorate], Guanyu banli qinfan gongmin geren xinxi xingshi anjian shiyong falü ruogan wenti de jieshi (关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) [Interpretation of Several Issues Concerning the Application of Laws in Handling Criminal Cases Infringing Citizens' Personal Information], https://www.spp.gov.cn/zdgz/201705/t20170510_190150.shtml (stating that "many cases of the leakage of citizens' personal information is committed by insiders (*neibu renyuan*)" emphasizing private actors, some of whom operate from within companies, banks, and other financial establishments).

[94] Zhonghua renmin gongheguo minfadian (中华人民共和国民法典) [Civil Code of the People's Republic of China], promulgated by the NPC on May 28, 2020 and effective January 1, 2021,

legislation is being drafted for review at the next meeting of the NPC, included the Personal Information Protection Law (*Geren xinxi baohufa*) and the Data Security Law (*Shuju anquanfa*), which will continue to shape the applicable rules governing the use of personal information.[95]

China's data governance regime emphasizes territoriality. This contrasts with the GDPR, which asserts jurisdiction over the processing of European personal data, regardless of where such processing takes place.[96] The GDPR applies to any data controller established within the EU and even to those not established in the EU, if they are offering goods or services or monitor the behavior of data subjects in the EU. These jurisdictional features contribute to the GDPR's global reach. In contrast, the PRC's Cybersecurity Law does not feature such "extraterritorial" elements; its application is confined to the "construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management *within the mainland territory* of the People's Republic of China."[97] The only explicit "extraterritorial" element in the Cybersecurity Law concerns the state's responsibility to monitor, prevent, and handle cybersecurity risks and threats arising from both within and *outside of* the mainland territory of the PRC.[98] In other words, while the territoriality of data storage and processing is largely immaterial for the GDPR's scope of application, it remains the central criterion for China's Cybersecurity Law.

Unlike the U.S., China used to be averse to the "extraterritorial" application of its domestic law.[99] This may be for historical reasons,[100] but may also stem from China's foreign policy, which has traditionally emphasized non-intervention.[101] The recent draft of the PRC's Data Security Law, however, features language that expands on the formulation in the Cybersecurity Law quoted above and appears to extend legal liability

---

https://www.pkulaw.com/chl/aa00daaeb5a4fe4ebdfb.html, art. 111 (stating that natural person's private information is protected by law).

[95] "Geren xinxi baohufa" zhongyu lai le! Zhe xie shiqing ni bixu zhidao (《个人信息保护法》终于来了! 这些事情你必须知道) [The "Personal Information Law" is Finally Here! These are Things You Certainly Must Know.] (May 26, 2020), https://baijiahao.baidu.com/s?id=1667730908978185466&wfr=spider&for=pc.

[96] GDPR, article 3.

[97] Cybersecurity Law, art. 2 (italics added for emphasis).

[98] Cybersecurity Law, art. 5.

[99] TONYA L. PUTNAM, COURTS WITHOUT BORDERS: LAW, POLITICS, AND US EXTRATERRITORIALITY (2016) (finding that for most of the post-World War II era, the U.S. has been a frequent regulator of activities outside its territory through its federal courts); KEVIN E. DAVIS, BETWEEN IMPUNITY AND IMPERIALISM: THE REGULATION OF TRANSNATIONAL BRIBERY 203–207 (2019) (describing how the US Foreign Corrupt Practices Act (FCPA) stretches the territoriality principle). *But see* William S. Dodge, *The New Presumption Against Extraterritoriality*, 133 HARV. L. REV. 1582 (2020) (describing the evolution of the presumption against extraterritoriality in US law).

[100] *See generally* Benjamin H. Williams, *The Protection of American Citizens in China: Extraterritoriality*, 16 AM. J. INT'L L. 43 (1922).

[101] MARC LANTEIGNE, CHINESE FOREIGN POLICY: AN INTRODUCTION 10 (2016); COURTNEY J. FUNG, CHINA AND INTERVENTION AT THE UN SECURITY COUNCIL: RECONCILING STATUS 2 (2019). *But see generally*, CHINA'S NEW ROLE IN AFRICAN POLITICS: FROM NON-INTERVENTION TO STABILIZATION? (CHRISTOF HARTMANN AND NELE NOESSELT, EDS., 2019) (documenting China's increasing engagement with African politics).

beyond the territory of mainland China.[102] Whether and how China will seek to effectuate such jurisdictional claims in future remains to be seen.[103] In any case, China's Cybersecurity Law as currently in force requires "territorial data localization": "critical information operators, " for example, Internet service providers (ISPs) and social media platforms, must store "personal information" or "important data" within China's mainland territory.[104] Territorial data localization is China's instrument of choice to assert "data sovereignty."

Territorial data localization has significant implications for foreign businesses in China that engage in cross-border business as they face steep compliance costs to onshore their data storage facilities, servers, and cloud-based servers within China, assuming they fall under the broad scope of "critical information operators."[105] Moreover, under the regulation on personal information flows, a transfer of important data outside of mainland China is only possible when "necessary" due to business requirements and subject to a security assessment.[106] Due to related time delays and costs, multinationals have adopted local storage and processing of data as a default solution.[107] The precise scope of China's territorial data localization requirement has been subject to much debate due to the inherent ambiguity in the Cybersecurity Law and its implementing specifications.[108]

---

[102] Draft Data Security Law, art. 2: Where organizations or individuals *outside of the mainland territory* of the People's Republic of China engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations of the People's Republic of China, *legal liability will be investigated according to the law*. (emphasis added). *See* Samm Sacks et al., *Five Important Takeaways From China's Draft Data Security Law*, NEW AMERICA (Jul. 9, 2020), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/. *Accord* Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region, promulgated by the National People's Congress Standing Committee on Jun. 30, 2020, art. 38 stating "This Law shall apply to offenses under this Law committed against the Hong Kong Special Administrative Region from outside the Region by a person who is not a permanent resident of the Region."

[103] China reportedly issued arrest warrants against US citizens from Hong Kong for violations of the newly imposed National Security Law, which also deploys extraterritorial language; *see* Samuel Chu, *We're All Hong Kongers Now*, NY TIMES (Aug. 10, 2020), https://www.nytimes.com/2020/08/10/opinion/china-hong-kong-arrest.html.

[104] Cybersecurity Law, art. 37.

[105] *See* Ge ren xinxi chujing anquan pinggu banfa (zhengqiu yijian gao) (个人信息出境安全评估办法（征求意见稿）) [Measures for Security Assessment for Cross-Border Transfer of Personal Information (Draft for Comment)], issued by the Cyberspace Administration of China on June 13, 2019, art. 3, http://www.cac.gov.cn/2019-06/13/c_1124613618.htm (hereinafter, "Measures for Security Assessment").

[106] Xinxi anquan jishu – ge ren xinxi anquan guifan (信息安全技术—个人信息安全规范) [Information Security Technology – Personal Information Security Specification] (promulgated by the Nat'l Info. Sec. Standardization Technical Comm on Dec. 29, 2019, effective June 1, 2018), https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf, art. 8(7).

[107] *See* Measures for Security Assessment *supra* note 105.

[108] *See e.g.*, Communication from the United States, Measures Adopted and Under Development by China Relating to its Cybersecurity Law, WORLD TRADE ORGANIZATION, https://perma.cc/4KE7-27FM (stating that the Cybersecurity Law's provisions on data localization have "significant adverse effect on trade in services"). *But see* Li Yi [李毅] & Wang Di [王迪], *Shimao zuzhi beijing xia Zhongguo shuju bendihua cunchu yaoqiu de pingxi [A Critique of China's data localization requirements under the WTO]*, 4 CHONGQING YOUDIAN DAXUE XUEBAO (SHEHUI KUEXUEBAN) [CHONGQING POST AND TELECOMMUNICATIONS JOURNAL (SOCIAL SCIENCE EDITION)] 34 (2019) (arguing that China's data localization requirements are in line with its WTO commitments).

China's data localization requirement addresses not only "where" data is stored and processed but also "by whom." It mandates that the relevant physical infrastructures (e.g., data centers) be geographically located in mainland China, and, ownership and control over such infrastructures by Chinese entities.[109] Despite the financial and reputational costs of these demands, some multinational corporations are unwilling to forego the Chinese market, even if they continue to have qualms about data localization.[110] For example, Apple was forced to host Chinese users' iCloud accounts in data centers located in mainland China through a Chinese partner company – AIPO Cloud (Guizhou) Technology Co. Ltd. (GCBD) to comply with the Cybersecurity Law.[111] Similarly, the world's leading cloud provider Amazon Web Services (AWS) was forced to divest itself from operating certain physical infrastructure in China.[112] Controversially, the data localization requirement also applies to the encryption keys through which encrypted data stored in the cloud can be decrypted.[113] Not only are multinationals required to store their data within China but their service providers, including foreign law firms, who have access to their confidential information, also face such requirements.[114]

While some have warned about potential spillover effects of China's territorial data localization demands, for instance, when U.S. user accounts inadvertently end up on Chinese servers,[115] such spillovers are arguably not preordained by law. In other words, it is possible for global technology companies to comply with China's data governance regime only within mainland China while operating differently elsewhere. This is crucial because it limits the global application of China's data governance framework. An incident involving the video communication company Zoom during the coronavirus pandemic is instructive in this regard: Chinese authorities notified Zoom about four

---

[109] Data center services require an Internet Data Centre Value Added Telecom Service license (IDC VATS) that is unavailable to foreign companies; *see* DLA Piper, *China: Regulation of Cloud Services in China – What Does it Mean for Your China Business?* (Dec. 28, 2016), https://blogs.dlapiper.com/privacymatters/china-regulation-of-cloud-services-in-china-what-does-it-mean-for-your-china-business/.

[110] U.S.-China Business Council, *Technology Security and IT in China: Benchmarking and Best Practices* 2 (2016), https://perma.cc/L772-WSX8 (finding that 43% of its corporate members were "very concerned" about Chinese policies on information flows and technology security). As an exception, Google famously left the Chinese market; *see* Henry Gao, *Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS*, 6 ASIAN J. WTO & INT'L HEALTH L & POL'Y 349 (2011) (examining whether China's censorship demands are in line with its commitments under WTO law).

[111] Apple Support, *Learn More About iCloud in China Mainland*, APPLE (May 26, 2020), https://support.apple.com/en-us/HT208351 (last visited Aug. 17, 2020).

[112] Jon Russell, *Apple's China iCloud Data Migration Sweeps up International User Accounts*, TECHCRUNCH (Jan. 11, 2018), https://techcrunch.com/2018/01/11/apple-china-icloud-international-users/.

[113] Stephen Nellis and Cate Cadell, *Apple Moves to Store iCloud Keys in China, Raising Human Rights Fears*, REUTERS (Feb. 24, 2018), https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060.

[114] These requirements extend to foreign law firms with a Chinese office. In the face of U.S. lawyers' duty of attorney-client confidentiality, they may face pressure by PRC law enforcement officers to hand over clients' information. This observation is based on one author's […] experience practicing law in Beijing.

[115] *See* Aynne Kokas, *Cloud Control: China's 2017 Cybersecurity Law and its Role in US Data Standardization* (Jul. 26, 2019), available at SSRN https://ssrn.com/abstract=3427372; Aynne Kokas, *Platform Patrol: China, the United States, and the Global Battle for Data Security*, 77 J. ASIAN STUD. 923 (2018).

upcoming commemorative meetings of the Tiananmen Square protests, and demanded termination of the meetings and host accounts to enforce Chinese law. Zoom sought to ascertain whether participants were physically present in mainland China and hence subject to the PRC's territorial jurisdiction. It shut down the meetings for which Zoom had circumstantial evidence of users being in mainland China and terminated the host accounts. This act of censorship, however, had extraterritorial effects because several hosts were based outside mainland China (one in Hong Kong, four in the U.S.). Zoom later apologized and promised to develop technology that would allow it to block individual users based on geographical location instead of creating extraterritorial spill-over effects by closing the whole meeting.[116]

These struggles reflect the tradeoffs involved when governments try to exercise jurisdictional control over data while accommodating commercial interests in cross-border data flows. This tradeoff is also visible in the EU where the GDPR limits the transfer of personal data from the EU to third countries.[117] The EU Court of Justice's decision in July 2020 to invalidate the Privacy Shield, which enabled the cross-border flow of personal data from the EU to the U.S. calls into question how the EU's insistence on fundamental rights protections can be reconciled with U.S. surveillance activities.[118] The EU's adequacy assessments create incentives for other countries to model data protection laws after the GDPR, thereby de facto increasing its jurisdictional reach.[119]

The EU is not alone in leveraging its legal system to entice convergence towards its laws. The U.S. CLOUD Act, which regulates transnational access to data for law enforcement, foresees that the U.S. can only enter into agreements with other countries with "robust substantive and procedural protections for privacy and civil liberties" akin to those favored by the U.S.[120] The CLOUD Act amended the Stored Communications Act to resolve the dispute between the U.S. federal government and Microsoft about

---

[116] Zoom, *Improving Our Policies as We Continue to Enable Global Collaboration* (Jun. 11, 2020), https://blog.zoom.us/improving-our-policies-as-we-continue-to-enable-global-collaboration/.

[117] GDPR, art 44.

[118] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020). *See* Henry Farrell & Abraham L. Newman, *Schrems II Offers an Opportunity—If the U.S. Wants to Take It*, LAWFARE (July 28, 2020), https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it (arguing that the US needs provide for cross-national protection of rights to enable data flows with Europe). *Contrast* Kenneth Kropp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (July 17, 2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision (arguing that the EU needs to change course to avoid isolation).

[119] In the absence of such convergence, companies may resort to data localization to avoid the strictures the EU imposes on cross-border transfers of personal data. *See generally* Anupam Chander, *Is Data Localization a Solution for Schrems II?*, 23 J OF INT'L ECON LAW 771 (2020) (arguing that data localization is only feasible for certain companies and ultimately undesirable).

[120] As the DOJ explains in its CLOUD Act white paper, relevant criteria include adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Budapest Convention; respect for the rule of law and principles of nondiscrimination; adherence to applicable international human rights obligations; clear legal mandates and procedures governing the collection, retention, use and sharing of electronic data; mechanisms for accountability and transparency regarding the collection and use of electronic data; and a demonstrated commitment to the free flow of information and a global Internet.

governmental access to data stored on Microsoft's servers in Ireland.[121] Microsoft argued that an assertion of extraterritorial jurisdiction (without additional safeguards) by the U.S. would negatively impact its transnational business relationships. The CLOUD Act does not seem to have dispelled these concerns fully as companies may face competing demands under the GDPR.[122]

The PRC's data governance regime does not feature comparable instruments of influencing other countries' data governance frameworks through legal requirements. But its attempt to reconcile governmental control over data flows with the rapid development and deployment of digital technologies seems to appeal to governments in emerging economies. This "pull" is the key driver of the Beijing Effect. It is complemented by a Chinese "push" through certain global data governance institutions to which we turn now.

C. China's Evolving Role in Global Data Governance Institutions

Domestic data governance frameworks are also influenced by international agreements and institutions. China has gradually adapted to the complicated institutional landscape of Internet governance that has been largely created and shaped by U.S. stakeholders and has been historically contested for this reason.[123] While continuing to participate in the established institutions, China created its own venue to advance Internet policy. China has consistently articulated a vision for global Internet governance that emphasizes governmental control over data flows under the rubric of "cyber sovereignty" and, more recently, "data sovereignty." China's multilateral forums with host states of the BRI also amplify these approaches, particularly in developing countries. This reflects a gradual shift from selective adaption to selective reshaping as China begins to assume a more assertive and pro-active role in global economic governance.[124] However, while China has embraced instruments of international economic law – free trade agreements and bilateral investment treaties – as a foundation for its trade and investment relations in principle, it has mostly refrained from advancing its data governance regime through trade agreements.[125] This stands in stark contrast to the U.S. and, to a lesser extent the EU, which seek to advance their data governance frameworks transnationally through formal instruments of international law.

---

[121] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), vacated and remanded sub nom. United States v. Microsoft Corp., 138 S. Ct. 1186, 200 L. Ed. 2d 610 (2018).

[122] *See* European Data Protection Supervisor and European Data Protection Board, Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence (Jul. 10, 2019), https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf.

[123] *See* ANDY RUSSELL, OPEN STANDARDS AND THE DIGITAL AGE: HISTORY, IDEOLOGY, AND NETWORKS (2014); LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE (2014).

[124] Pitman B. Potter, *Globalization and Economic Regulation in China: Selective Adaptation of Globalized Norms and Practices*, 2 WASH. U. GLOBAL STUD. REV. 119 (2003); Heng Wang, *Selective Reshaping: China's Paradigm Shift in International Economic Governance*, 23 J. OF INTL. ECON. LAW (Forthcoming) (2020).

[125] *See infra* note 132.

Under the Obama administration, the U.S. developed a new template of rules for the digital economy with an emphasis on provisions that require a legitimate public policy objective for measures that restrict the free flow of information or that require the use of domestic computing facilities, subject to a three-prong test of non-discrimination/arbitrariness, trade restrictiveness, and, most importantly, necessity. Despite the U.S.' ultimate withdrawal from the Trans-Pacific Partnership (TPP), the remaining eleven countries around the Pacific Rim, including China's neighbor, Vietnam, came to endorse these provisions and the "Silicon Valley Consensus" they represent in the resuscitated TPP, now known as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which limits these states' ability to follow China's data governance model.[126] Some CPTPP members are also BRI countries.[127] They participate in two different forms of "megaregional" ordering.[128] On the one hand, it may be possible for the CPTPP members to reconcile their commitments in favor of cross-border data transfers and against territorial data localization under the CPTPP with their economic relationship with the PRC under the BRI, because the latter does not impose a certain data governance model on host countries. On the other hand, countries conducive to the Beijing Effect that want to emulate the PRC's "data sovereignty" approach will want to refrain from entering into CPTPP-style commitments.

Similarly, due to concerns that commitments for free data flows and against data localization requirements in trade agreements would be mobilized against its data protection regime, the EU opposed such language in its failed trade negotiations with the U.S. on the Trans-Atlantic Trade and Investment Partnership (TTIP) and the stalled trade in services agreements (TISA). Eventually, the EU developed a new template to reconcile its interest in free data flows with its concerns over data protection and privacy. These rules (only) ban de jure data localization (not restrictions of cross-border data flows as under GDPR) and carve out data protection and privacy from scrutiny by state-dispute settlement or investment arbitration panels.[129] The template is designed to compel the EU's trading partners to sign on to the EU's conception of data protection and privacy as fundamental rights.[130] In addition, the EU's fraternal twin, the Council of Europe, has advocated for a similarly human rights-based data protection approach through its

---

[126] Thomas Streinz, *Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy*, *in* MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP (Benedict Kingsbury et al. eds., 2019), ch. 14.

[127] *See Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Accession Process*, https://perma.cc/8TX7-UXDF, last visited Aug. 17, 2020. Of the states that have ratified the CPTPP, New Zealand, Singapore, and Vietnam have all signed international agreements under the BRI. *See Belt and Road Portal*, https://eng.yidaiyilu.gov.cn/info/iList.jsp?cat_id=10076, last visited Aug. 17, 2020. Singapore also created an Electronic Origin Data Exchange System with China, https://www.customs.gov.sg/businesses/certificates-of-origin/eodes-with-china.

[128] *See* Jing Tao, *TPP and China: A Tale of Two Economic Orderings?, in* MEGAREGULATION CONTESTED: GLOBAL ECONOMIC ORDERING AFTER TPP (Benedict Kingsbury et al, eds. 2019) ch 4.

[129] *See supra* note 126.

[130] EU Template for Horizontal Provisions for Cross-Border Data Flows and for Personal Data Protection in EU Trade and Investment Agreements, https://perma.cc/KSQ2-T4MW. In the EU-UK Trade and Cooperation Agreement, article DIGIT.7.1, the UK was only willing to affirm that individuals have "a right" to data protection and privacy.

"Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," which is open for non-European countries to join.[131]

In contrast, until recently, China's free trade agreements either did not address data governance questions at all (as in the case of the 2006 China-Pakistan agreement) or used very weak and ultimately inconsequential language (as in the 2012 China-Australia agreement).[132] In November 2020, however, China signed the Regional and Comprehensive Economic Partnership (RCEP) agreement.[133] RCEP's e-commerce chapter is modeled after CPTPP's but allows countries to self-assess which data transfer restrictions and data localization requirements are necessary.[134] In the World Trade Organization (WTO), China has advanced a conception of "electronic commerce" that emphasizes the role digital technologies play in facilitating the trade of goods and services via online platforms such as Alibaba's. While China recognizes the significance of data flows for trade and development and participates in the WTO's efforts to create new plurilateral rules for electronic commerce, it maintains that "the data flow should be subject to the precondition of security" which necessitates, in China's view, "that the data flow orderly in compliance with [WTO] Members' respective laws and regulations."[135]

While taking a defensive position in trade negotiations, the PRC has become increasingly active in promoting its conception of data governance in various Internet governance institutions. These include organizations with erstwhile predominantly Western participation such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), as well as UN entities such as the International Telecommunication Union (ITU).[136] China's membership and increasing participation in such forums is part of its broader agenda to integrate its norms

---

[131] Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay have joined the 47 Council of Europe members in ratifying the Convention. *See* Council of Europe, *Details of Treaty No. 108*, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, last viewed Aug. 17, 2020.

[132] Australia-China FTA, article 12.8.1 reads, "Notwithstanding the differences in existing systems for personal information protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal information of users of electronic commerce." *See* Gao *supra* note 82 (noting that of China's FTAs, only its FTA with Korea and Australia contain stand-alone chapters on e-commerce).

[133] RCEP was signed between the ten ASEAN members and their major trading partners China, Japan, South Korea, Australia, and New Zealand, after India had departed the negotiations. *See* Pasha L. Hsieh, *Against Populist Isolationism: New Asian Regionalism and Global South Powers in International Economic Law*, 51 CORNELL INTL L J 683 (2018).

[134] Contrast RCEP, article 12.14 and 12.15 (including corresponding footnotes 12 and 14) with CPTPP, articles 14.11 and 14.13.

[135] WTO Joint Statement on Electronic Commerce: Communication from China, INF/ECOM/19 (Apr. 24, 2019), 4.3. *See* Henry Gao, *Across the Great Wall: E-Commerce Joint Statement Initiative Negotiation and China* (draft manuscript, on file with authors).

[136] *See* Jonathan E. Hillman, "A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards," *Statement before the U.S.-China Economic Security Review Commission*, https://www.uscc.gov/sites/default/files/Jonathan%20Hillman%20Written%20Testimony%203.13.20.pdf (last visited Aug. 17, 2020) (arguing that China has pushed for standards strengthening the role of governments at the ITU).

into the main institutions of global governance.[137] China consistently promotes a strong role of the state in setting Internet policy along the lines of cyber sovereignty and data sovereignty at the expense of freedom of expression and civil society participation.[138]

Another way in which China has been promoting its values in global governance is by creating parallel institutions to those mainly established by the U.S. These include the Shanghai Cooperation Organization, the Asian Infrastructure Investment Bank, the Silk Road Fund, and its own system of development finance and overseas aid.[139] Data governance is no exception in this regard. Whereas China has been particularly active in the UN system in promoting its view of cyber sovereignty through the Group of Government Experts (GGE), it has also encountered U.S. resistance and hence in 2018, China, along with Russia, and other like-minded countries founded an alternative platform to the GGE—the Open Ended Working Group (OEWG).

Furthermore, since 2014, the CAC and the People's Government of Zhejiang Province have been co-hosting the "World Internet Conference" (*Shijie hulianwang dahui*) also called the "Wuzhen Summit" in Wuzhen, Zhejiang, the province that is the birthplace of Alibaba. In contrast to established Internet governance fora, which are generally open, China banned certain Western journalists from the event. Based on official Chinese information, the Wuzhen Summit has grown over the years from 100 attendees in 2014 to 1,500 in 2019, including Internet experts, government officials, and technology entrepreneurs, from both developing and developed countries.[140] The extent to which the presence of representatives of other Internet governance institutions might lend legitimacy to the event has been controversial.[141] The Wuzhen Summit has been a vehicle for China to popularize its vision for the Internet, including cyber sovereignty.[142] China's discursive "soft power" does not only filter through such China-based platforms but also through other bilateral and multilateral meetings, including the China-US Internet Forum, China-UK Internet Roundtable, China-ASEAN Information Port Forum, China-Arab Countries Online Silk Road Forum, and the China-Singapore Internet

---

[137] Ann Kent, *China's Participation in International Organizations*, *in* POWER AND RESPONSIBILITY IN CHINESE FOREIGN POLICY 132, 133 (Yongjin Zhang & Greg Austin eds., 2013) (observing China's steady involvement in international organizations, including some 50 by 2000); CONGYAN CAI, THE RISE OF CHINA AND INTERNATIONAL LAW: TAKING CHINESE EXCEPTIONALISM SERIOUSLY 162 (2017) (providing a typology of China's engagement with international organizations); Kristine Lee, *It's Not Just the WHO: How China is Moving on the Whole U.N.* POLITICO (April 15, 2020), https://www.politico.com/news/magazine/2020/04/15/its-not-just-the-who-how-china-is-moving-on-the-whole-un-189029 (noting, "Beijing has systematically positioned Chinese nationals at the head of a wide range of U.N. agencies").

[138] *See* Hillman *supra* note 136 at 6-7.

[139] *See* Erie *supra* note 1.

[140] World Internet Conference, *Wuzhen Summit*, http://www.wuzhenwic.org/aboutwic.html (last visited Aug. 12, 2020).

[141] *See* Milton Mueller, *The Wuzhen Compradors*, INTERNET GOVERNANCE PROJECT (Dec. 29, 2015), https://www.internetgovernance.org/2015/12/29/the-chinese-netmundial-initiative/ (arguing for engagement with China on Internet governance topics but against support for CCP sponsored event).

[142] *See e.g.*, Zhou Lanxu and Wang Ying, Sovereignty in Cyberspace *Paper Unveiled*, CHINA DAILY (Oct, 22, 2019), http://www.wuzhenwic.org/download/CHN-BRO-Life-00222.pgl.pdf (defining cybersovereignty as "facilitating a just and equitable international cyberspace order on the basis of national sovereignty").

Forum.[143] Collectively, then, such forums promote China's selective reshaping of data governance.[144] China's discursive reshaping my further assume normative form, such as in the "International Strategy on Cooperation on Cyberspace" of 2017, which identifies "sovereignty" (*zhuquan*) as a cornerstone for international coordination on cyber issues.[145] In September 2020, China proposed a Global Data Security Initiative, which urges respect for countries' sovereignty, jurisdiction, and data management rights.[146]

In summary, while China has refrained from using international law to export its approach to domestic data governance to other countries (as the U.S. and, to a lesser extent, the EU have done), it is playing an increasingly assertive role in existing and newly established global data governance institutions. These institutions may be broadly discursive; they show how China both operationalizes existing institutional channels and sometimes creates its own to socialize foreign actors into its own approach. Further, some of these institutions play a crucial role in defining the standards for digital infrastructure, which is one reason for the increasing importance of China in infrastructural data governance, a topic to which we now turn.

D. China's Increasing Importance in Infrastructural Data Governance

Infrastructural data governance highlights the extent to which the regulation of data flows is a function of the physical, digital, and platform infrastructures that shape the digital domain. To note, all digital infrastructures rely on non-digital infrastructures. Data is not stored in an ephemeral "cloud" but on hard drives in data centers. As Tung-Hui Hu explains: "We may imagine the digital cloud as placeless, mute, ethereal, and unmediated. Yet the reality of the cloud is embodied in thousands of massive data centers, any of which can use as much electricity as a midsized town."[147] When data "flows" through the Internet, the packets of zeros and ones are being carried through copper or fiber-optic cables or are being transmitted through electromagnet radiation via routers that create local-area networks ("WiFi") or via antennas that build cell phone networks.[148] Without these materials components and related infrastructures (e.g., electricity), data cannot be stored, processed, or transferred. This may seem basic but is fundamental for developing countries with embryonic digital infrastructures. As we show, one central reason for China's growing influence in transnational data governance is that Chinese technology companies are increasingly developing, supplying, and maintaining the physical components on which digital infrastructures rely.[149]

---

[143] *See supra* note 86.
[144] *See* Sarah McKune and Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMM'S 3835 (2018).
[145] *Wangluo kongjian guoji hezuo zhanlüe* (网络空间国际合作战略) [International Strategy on Cooperation on Cyberspace] (Mar. 1, 2017), Ch. 2.2, http://www.81.cn/jmywyl/2017-03/01/content_7509042.htm.
[146] Zhonghua renmin gongheguo waijiaobu (中华人民共和国外交部) [PRC Ministry of Foreign Affairs] Quanqiu shuju anquan changyi (全球数据安全倡议) [Global Data Security Initiative], Sept. 8, 2020, https://www.fmprc.gov.cn/web/wjbzhd/t1812947.shtml.
[147] TUNG-HUI HU, A PREHISTORY OF THE CLOUD (Abstract) (2015).
[148] *See* James Grimmelmann, INTERNET LAW: CASES AND PROBLEMS 27-32 (10th ed., 2020).
[149] *See infra* §III.

In addition to physical components, data transmissions rely on standardized protocols. Internet-networking is made possible by the fundamental Internet protocols. Even countries, such as China, which restrict cross-border data flows through dedicated data control infrastructures, rely on these protocols. They also generally comply with the ICANN-run domain name system (DNS) that ensures that each node of the Internet is uniquely identifiable by a "number" (the IP address), which corresponds to an equally uniquely identifiable "name" (the domain name).[150] In other words, China's data control infrastructure is compatible with the Internet's core infrastructure.

There is no need for China – or any other country, for that matter – to meddle with the Internet's fundamental protocols to assert control over domestic or transnational data flows.[151] However, that does not mean that exercising such control is straightforward. What is colloquially known as the "Great Firewall" of China (GFW) is in reality a complex data control infrastructure that combines various legal and technical means to assert the desired extent of control, which is even in the case of the PRC, far from absolute.[152] The GFW controls traffic at it moves from the global Internet into China and monitors data flows between Chinese ISPs.[153] Where China's network interconnects with other networks, the GFW is comprised of software that filters every packet of data for prohibited content.[154] Internally, when a user attempts to load a webpage, their ISP will ping a list of forbidden URLs; in the event that the user's request is not banned, the request is forwarded to an Internet access point (IAP), which handles routing traffic to servers in China.[155] Critically, the IAPs are limited by the physical infrastructure, in this case, a fiber-optic network with three chokepoints at which data flows can be blocked.[156] This infrastructure has been seen as a template for other states that share Beijing's twin priorities of national security and digital commerce.

Foreign companies respond to China's data flow control infrastructure by segmenting their products. Occasionally, these efforts at "geofencing" – the corollary to data localization – fail and data gets inadvertently routed through mainland China and becomes exposed to PRC monitoring. When the coronavirus pandemic forced Western countries into lockdown in the spring of 2020, and demand for Zoom skyrocketed, Zoom

---

[150] *See* Milton L. Mueller, *China and Global Internet Governance: A Tiger by the Tail, in* ACCESS CONTESTED: SECURITY, IDENTITY AND RESISTANCE IN ASIAN CYBERSPACE (Ronald Deibert, et al, eds., 2011).
[151] Huawei caused controversy by proposing the development of new Internet protocol standards (misleadingly called "New IP") in a white paper directed at the ITU's standard-setting community. *Compare* Anna Gross & Madhumita Murgia, *China and Huawei propose reinvention of the internet* (FINANCIAL TIMES, Mar. 27, 2020), *with* Milton Mueller, *About that Chinese "reinvention" of the Internet…* (INTERNET GOVERNANCE PROJECT, Mar. 30, 2020), https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/.
[152] *See* Richard Clayton, Steven J. Murdoch, and Robert N.M. Watson, *Ignoring the Great Firewall of China, in* PRIVACY ENHANCING TECHNOLOGIES (George Danezis & Philippe Golle, eds., 2006).
[153] James Griffith, THE GREAT FIREWALL IN CHINA: HOW TO BUILD AND CONTROL AN ALTERNATE VISION OF THE INTERNET Ch. 2 (2019).
[154] *Id.*
[155] *Id.*
[156] *Id.*

had to scale up its cloud infrastructure and inadvertently added data centers in China as backup, which led to data flows of Zoom meetings involving users outside China being routed through mainland China.[157] Concerns about increased routing of data flows through Hong Kong due to increased bandwidth and reduced latency also prompted the US government to force Google and Facebook to abandon its plans to include Hong Kong into its Pacific Light Cable Network that connects Los Angeles to the Philippines and Taiwan.[158]

Beyond data flow control infrastructures, the standardization of new transmission protocols has attracted much attention and, as a result, generated considerable geopolitical tensions. The fifth generation standard for transmission of data through cellular networks ("5G") marks arguably the first time during the Internet era that Chinese companies enjoy technological and commercial leadership.[159] This expertise and commercial power translates naturally into considerable influence in international technical standard-setting bodies, which can amplify standards globally.[160] However, the growing design power of Chinese technology companies materializes even without the endorsement of the global community of technical standard-setters. If Chinese technology companies build equipment according to a certain standard and export this equipment to other countries, the standards embedded in the products get exported as well. This basic insight is true not only for cellular networks and their technical standards; it also applies to other digital infrastructures, for example the surveillance technology deployed in inter-connected "smart" cities.[161]

When infrastructures regulate, it is not just because of their physical components or their standards and protocols.[162] Infrastructures are more than their constitutive parts. It is ultimately humans in their respective organizational contexts – whether governmental or commercial – that develop, build, configure, maintain, interrupt, or even destroy digital infrastructures. In other words, the political cannot be divorced from the infrastructural. Territorial control over the physical components of digital infrastructure in itself is insufficient to control data flows domestically or across borders. A government that aspires towards "data sovereignty" needs control over the entities that fulfill these infrastructural functions. Hence, the fact that digital infrastructures are increasingly supplied by Chinese technology corporations poses distinct challenges due to their

---

[157] Bill Marczak and John Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings,* CITIZEN LAB (Apr. 3, 2020), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/. Eric S. Yuan, *Response to Research From University of Toronto's Citizen Lab,* ZOOM (Apr. 3, 2020), https://blog.zoom.us/response-to-research-from-university-of-torontos-citizen-lab/.

[158] *See* Todd Shields, *Google, Facebook Dump Plans for U.S.-Hong Kong Undersea Cable*, BLOOMBERG (Aug. 28, 2020), https://www.bloomberg.com/news/articles/2020-08-29/google-facebook-dump-hong-kong-cable-after-u-s-security-alarm.

[159] *See* Paul Triolo et al., *Eurasia Group White Paper: The Geopolitics of 5G*, EURASIA GROUP (Nov. 15, 2018), https://perma.cc/72BS-54W4.

[160] *See* Bureau of Industry and Security, Commerce, Temporary General License (May 22, 2019), https://www.federalregister.gov/documents/2019/05/22/2019-10829/temporary-general-license (authorizing engagement with Huawei for purposes of 5G standard-setting).

[161] *See infra* §IV.B.

[162] *See supra* text accompanying notes 36–39.

intricate relationship with the CCP.[163] Consequently, it may be difficult for foreign jurisdictions, especially developing countries, to assert effective jurisdictional control over Chinese technology companies, whether state-owned or (formally) private.[164]

Platforms with infrastructural characteristics are important venues of global data governance conducted by corporations.[165] The growing influence of Chinese companies over telecommunications and e-commerce platforms outside China is thus a key driver of the Beijing Effect. Platforms are targets for governmental demands to censor speech or to provide access to data but their regulatory ambit extends beyond their role as intermediaries for public data governance. Social media platforms in particular have emerged as "new governors" of speech and data around the world.[166] They enjoy considerable freedom, on the basis of contractual user consent to their terms of service, backed by protections against liability in many jurisdictions, and only imperfectly constrained by data protection and privacy laws, to decide which content to allow and which data to collect. US platforms such as Facebook have sought to orient themselves towards US free speech values and international human rights standards in their content moderation practices and attracted much criticism for their handling of misinformation and harmful (but not illegal) content.[167] Chinese platforms such as TikTok face similar and choices in their operations around the globe.[168] TikTok maintains that it does not remove content on its US platform based on sensitivities related to China,[169] but its moderation guidelines appear to ban "highly controversial topics, such as separatism, religion sects conflicts, conflicts between ethnic groups, for instance exaggerating the Islamic sects conflicts" which accords with the PRC campaign against the Uyghurs in Xinjiang.[170] Infrastructural data governance is shaped by corporate compliance with domestic and international law, but is also determined by the choices that platforms make in the absence of legal demands and in response to ethical, political, or market pressures.

To summarize, China has growing influence in infrastructural data governance because Chinese technology companies increasingly supply the relevant physical

---

[163] *See infra* text accompanying notes 194–203.
[164] *See infra* text accompanying notes 190–192.
[165] Jean-Christophe Plantin et al., *Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook*, NEW MEDIA & SOCIETY 1 (2016) (explaining how platforms enable and constrain new digital services that acquire characteristics of infrastructure).
[166] Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2017); Rebecca Hamilton, *Governing the Global Public Square,* HARV. INTL. L. J. (forthcoming 2021).
[167] *Id. See also* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report on content regulation* (Apr. 6, 2018), A/HRC/38/35.
[168] For example, TikTok's content moderation practices have been criticized for suppressing posts by "ugly" and poor people to attract new users; Sam Biddle, Paul Victor Ribeiro, and Tatiana Dias, *Invisible Censorship: TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users*, THE INTERCEPT (Mar. 16, 2020), https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.
[169] Statement on TikTok's Content Moderation and Data Security Practices (Oct. 24, 2019), https://newsroom.tiktok.com/en-us/statement-on-tiktoks-content-moderation-and-data-security-practices.
[170] Lily Kuo, *TikTok 'Makeup Tutorial' Goes Viral with Call to Action on China's Treatment of Uighurs*, THE GUARDIAN (Nov. 27, 2019), https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs (citing leaked moderation guidelines).

components of digital infrastructures, set the relevant standards (both domestically and internationally), and operate and control digital platform infrastructures outside China. All these elements are present in the DSR and contribute to the Beijing Effect.

III. China's Digital Silk Road

When most people hear "Belt and Road Initiative" (BRI), they think of highways, dams, and economic corridors. The Digital Silk Road (DSR) is a largely overlooked but no less fundamental part of the larger BRI, and one that may gain even greater importance in the post-COVID future. The DSR is driven by the globalization of China's telecommunications and e-commerce companies. This form of globalization envisions China as the epicenter of a new global digital economy and seeks to build digital infrastructures for development. The DSR promotes digital inter-connectiveness between national economies to facilitate transnational economic linkages. Chinese companies' digital globalization has received strong backing from the central government. The DSR dovetails with such initiatives as the "Made in China 2025" plan, which aims to drive China up the global value chain by producing "smart" manufacturing, and which in 2020 received a boost of $1.4 trillion.[171]

The DSR is a constitutive part of the BRI and shares many features with it. As with much BRI rhetoric, the concepts and definitions of the DSR have been in flux. Policy documents over the years have interchangeably used "information silk road" (*xinxi sichouzhilu*), "silk road online" (*wangshang sichouzhilu* or *hulian hutong zhi sichou zhilou*), and "digital silk road," with a consensus usage preferring the latter as of roughly 2017, the year of the first BRI Forum in Beijing. The DSR, like the BRI, shows a flurry of discourse production that can often obscure the actual operative mechanisms and reality on the ground.[172]

Official pronouncements on the DSR frequently make reference to "connectivity," perhaps one of the defining concepts for Chinese perceptions of its form of globalization. One reference point for this discourse is Xi Jinping's speech as the first BRI Forum, when he introduced the DSR. Xi urged participants "to pursue innovation-driven development and intensify cooperation in frontier areas such as digital economy, artificial intelligence, nanotechnology and quantum computing, and advance the development of big data, cloud computing and smart cities so as to turn them into a digital silk road of the 21st century."[173] The speech frequently uses what in English is translated as

---

[171] Jost Wübbeke et al., *Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries*, MERICS NO. 2 (Dec. 2016), https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf. (detailing China's efforts to catalyze its high-tech industries to reduce foreign dependence); Joe Devanesan, *Inside China's New $1.4 Trillion-Dollar Digital Transformation Master Plan,* TECHWIRE ASIA (May 29, 2020) https://techwireasia.com/2020/05/inside-chinas-new-us1-4-trillion-dollar-digital-transformation-master-plan/ (explaining how the capital injection was a response to the U.S. Government's blocking Chinese investment in the technology sector).

[172] *See infra* §IV.

[173] Xi Jinping, *Work Together to Build the Silk Road Economic and the 21st Century Maritime Silk Road*, BELT AND ROAD FORUM FOR INTERNATIONAL COOPERATION (May 14, 2017), http://www.chinadaily.com.cn/beltandroadinitiative/2017-05/14/content_29341195.htm.

"connectivity." However, this is a simplification of the original Chinese concept, which is polyvalent. The original Chinese, for example, uses terms such as "policy communication" (*zhengce goutong*), "infrastructural connectivity" (*sheshi liantong*), "trade unblocking" (*maoyi chantong*), "financial circulation" (*zijin rongtong*), and "popular sentiment interlinking" (*minxin xiangtong*).[174] All of these are translated, whether in official English versions of speeches or in the secondary literature, as "connectivity." The 2017 speech further mentions *hulian hutong*, alongside these other actions, a term translated as "cyberspace connectivity" but which more accurately means "cyberspace interoperability."[175] More precisely rectifying terms reveals that Xi's discourse of globalization to evoke an assemblage of interlocking unities, with cyberspace interoperability (not just connectivity) as one main mechanism for integration on the basis of common standards and digital infrastructures to share data between different systems. While the DSR has unique features it is not necessarily incompatible with existing digital infrastructures, may build open them, or lay the foundation for new ones. This nature of the DSR highlights the importance of technical standard-setting for determining upward and downward compatibility as well as interoperability between systems.[176]

Moving from discourse to operations, the two key elements of the DSR that generate the Beijing Effect are the investment in physical components of digital infrastructure such as terrestrial and submarine cables and a strong role for Chinese technology companies as providers of infrastructural services. As generally with the BRI, there is no formal treaty under international law to bind partner countries in their commitment to the DSR. Instead, the DSR operates under a complex web of nonbinding soft law instruments such as Memoranda of Understandings (MoUs) and policy documents. In the following, we address each of these features in turn.

A. Supplying Physical Components of Digital Infrastructure

The first main element of the DSR is the supply of physical components for digital infrastructures. As a 2015 white paper by China's National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce argues: "[China] should jointly advance the construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an information Silk Road."[177] The State Council's subsequent Five-Year Plan for National Economic and Social Development of 2016 dedicates a

---

[174] *Id.*
[175] *Id*.
[176] *See, e.g.,* John Seaman, *China and the New Geopolitics of Technical Standardization*, NOTES DE L'IFRI (Jan. 2020); Jeffrey Ding, *Balancing Standards: U.S. and Chinese Strategies for Developing Technical Standards in AI* (NBR.ORG, July 1, 2020), https://www.nbr.org/publication/balancing-standards-u-s-and-chinese-strategies-for-developing-technical-standards-in-ai/.
[177] Quoted in Keshav Kelkar, *From Silk Threads to Fiber Optics: The Rise of China's Digital Silk Road* OBSERVER RESEARCH FOUNDATION ONLINE, Aug. 8, 2018), https://www.orfonline.org/expert-speak/43102-from-silk-threads-to-fiber-optics-the-rise-of-chinas-digital-silk-road.

whole section to digital infrastructures.[178] It states the goals of establishing smooth international communication facilities, optimizing the layout of international communication networks, and improving cross-border land and sea cable infrastructure, mentioning a Sino-Arab "online Silk Road" alongside the "China-ASEAN Information Port," that was announced with great fanfare in 2015, although it does not seem to have progressed.[179] The uneven implementation of certain projects under the DSR is broadly representative of the BRI, at large, given the breadth and scope of the projects, many of which are located in and across challenging regulatory landscapes.

However, various cable projects by Chinese technology companies, both terrestrial and submarine, have been completed or are on schedule. Projects include: the Africa Europe-1 (AAE-1) submarine cable with participation by China Unicom; the submarine Bay of Bengal Gateway (BBG) and the Southeast Asia-Middle East-Western Europe submarine cable (SEA-ME-WE 5) across the Bay of Bengal, both with involvement of China Mobile; and, the submarine Pakistan East Africa Cable Express that Huawei Marine is pursuing and for which the Chinese Hengtong group is supplying the fiber optic cable, and two terrestrial cables, both with involvement of China Telecom: one between China (Kashgar) and Afghanistan (Faizabad) through the Wakhan region, the other between China (Jilongzhen) and Nepal (Rasuwagadi) outside Kathmandu.[180] China Mobile is also one of the companies behind the "2Africa" project, comprised of a 37,000 kilometer cable, one of the world's largest undersea cables, to be completed by 2024, linking Africa, Europe, and the Middle East.[181] Meanwhile, the Arctic Connect project seeks to link Europe and Asia through a new submarine communication cable along the Northern Sea Route (built by Huawei).[182] While fiber-optic cables remain the world's most important physical infrastructure for transnational data flows,[183] China has also shown interest in supplying Internet connectivity through space via low orbit satellites.[184]

---

[178] Zhonghua renmin gongheguo guomin jingji he shehui fazhan di shisan ge wunian guihua gangyao (中华人民共和国国民经济和社会发展第十三个五年规划刚要) [National Economic and Social Development of the PRC: Outline f the 13th Five Year Plan], issued by the Central Government of the PRC, Mar. 17, 2017, Part 7, http://www.gov.cn/xinwen/2016-03/17/content_5054992.htm.

[179] China-ASEAN Information Harbor Forum (Sept. 13-14, 2015), http://www.chinadaily.com.cn/business/informationharbor/index.html (last visited Aug. 17, 2020).

[180] *See* Cave et al. *supra* note 15.

[181] Anon., *China Mobile and Partners to Built Undersea Cable Connecting Africa and the Middle East*, GLOBAL TIMES (Jun. 15, 2020), https://www.globaltimes.cn/content/1188471.shtml.

[182] *See* Frank Juris, *Handling over infrastructure for China's strategic objectives: 'Arctic Connect' and the Digital Silk Road in the Arctic*, Policy brief presented at the conference "Beyond Huawei: Europe's adoption of PRC technology and its implications," Prague, Nov. 27, 2019.

[183] *See* SUBMARINE CABLES: THE HANDBOOK OF LAW & POLICY, 3 (Douglas R. Burnett et al., eds., 2014) (estimating that about 97% of international communications ran through submarine cables in 2014).

[184] *See* Ajey Lele and Kritika Roy, *Analysing China's Digital Space Belt And Road Initiative*, IDSA OCCASIONAL PAPER NO. 54, https://idsa.in/system/files/opaper/china-digital-bri-op55.pdf. The COVID-19 pandemic seems to have affected China's satellite manufacturing capacity in Wuhan; *see* Xinmei Shen, *Why the Coronavirus Slowed China's Plan to Take on Elon Musk's Internet Satellites*, ABACUS (Apr. 15, 2020), https://www.scmp.com/abacus/tech/article/3080118/why-coronavirus-slowed-chinas-plan-take-elon-musks-internet-satellites.

As part of the DSR, Chinese companies are building data centers in host states. In 2017, Alibaba Cloud established cloud computing big data hubs called "Flying Apsaras Data Centers" (*feitian shuju zhongxin*) in seventeen regions of the world, including in Malaysia, Indonesia, and Singapore, creating Asia's largest platform for cloud-based computing.[185] Not to be outdone, China Telecom Global is building data centers in BRI countries to house large-capacity servers and data storage systems to host cloud computing services.[186]

The DSR, then, is comprised of physical components necessary for managing, transferring, and storing of data. Chinese technology is both relatively cheap and mostly of high quality. The combination of these factors creates strong demand among DSR host states. However, cost competitiveness is only one and not necessarily the decisive factor that creates demand for Chinese technology.[187] In addition to cost, China's version of data sovereignty attracts decision-makers in certain host states. Importantly, the fiber optic cables, data centers, and satellites cannot operate by themselves. Most BRI deals, financed by Chinese development banks, require that Chinese contractors build and maintain the relevant infrastructure, and digital infrastructures are no exception.

B. Chinese Technology Companies as Infrastructural Agents

Chinese companies play a central role in the DSR. Hardware and software require not only installation but also maintenance[188] and under most BRI projects, Chinese companies have a near monopoly on providing these services.[189] Indeed, the DSR is to a certain extent equivalent to Chinese companies' global expansion strategies in sectors such as e-commerce, telecommunications, and research and development (R&D). Importantly, these services sectors are themselves *infrastructural* as they, respectively, enable other companies (both foreign and domestic) to benefit from selling goods and services via e-commerce and mobile payment platforms, by facilitating communication along local and cross-border supply chains, and by creating an environment of innovation

---

[185] Zhongguo IDC Quan (中国 IDC 圈), Shiqi daqushu shige feitian shuju zhongxin, Aliyun cheng Yazhou guimo zuida yun pingtai (17 个大区数十个飞天数据中心，阿里云成亚洲规模最大云平台) [With Dozens of Feitian Data Centers in 17 Regions, Alibaba Cloud Has Become the Largest Cloud Platform in Asia], IDC Xinwen (IDC 新闻) [IDC News], Jun, 16, 2017, http://news.idcquan.com/news/119002.shtml.

[186] Zen Soo, *China Telecom Global Sets Sights on Data Centres for Belt and Road Region*, SO. CH. MORNING POST (Apr. 25, 2017), https://www.scmp.com/tech/enterprises/article/2090533/china-telecom-global-sets-sights-data-centres-belt-and-road-region.

[187] Regarding broadband infrastructure, Chinese firms face competition from Sweden's Ericsson and Finland's Nokia, which are also active in emerging markets, although both seem to be losing ground to Huawei and ZTE. Juan Pedro Tomás, *Ericsson Targets Emerging Markets with New Suite of Solutions*, RCRWIRELESSNEWS (Sept. 14, 2016), https://www.rcrwireless.com/20160914/network-infrastructure/ericsson-targets-emerging-markets-tag23; Arthur D. Little, *Nokia Named Winning Emerging Market Player*, https://www.adlittle.co.uk/en/insights/press/press-release/arthur-d-little-nokia-named-winning-emerging-market-player (last visited Nov. 27, 2020).

[188] The maintenance of traditional infrastructure, while overshadowed by the media attention to the initiation of new construction projects, has more recently become the object of study. *See e.g.*, Agnieszka Joniak-Lüthi, *A Road, A Disappearing River and Fragile Connectivity in Sino-Inner Asian Borderlands*, 78 POL. GEOGRAPHY 102 (2020) (analyzing the difficulties in maintaining roads in Xinjiang).

[189] *See* Erie *supra* note 1.

and growth. A closer examination of the companies that are providing these digital services reveals how their relationship to the party-state enables the Beijing Effect.

The DSR is being built by both China's state-owned enterprises (SOEs) and large private multi-national corporations (MNCs) that, to varying degrees, exist in agent-principal relationships with the party-state, an organizational fact which has implications for data governance. Whereas the BRI has generally been spearheaded by China' major SOEs in construction, oil and gas, and steel, the DSR has, for the most part, been led by China's "private" tech companies such as Alibaba Group Holding Limited ("Alibaba"), Tencent Holding Limited ("Tencent"), Huawei Technologies Company Limited ("Huawei"), ZTE Corporation ("ZTE"), and J.D.com Incorporated ("Jingdong"). China's SOEs in telecommunications, that is, China Mobile, China Unicom, and China Telecom, also play a strong role. China's SOEs are not only commercial actors but also political ones that serve the geopolitical aims of the party-state.[190] The relationship between the MNCs and the party-state is less clear, and has become one of the most contentious issues in the U.S.-China trade conflict.[191]

Chinese enterprises, whether state-owned or private, are part of an ecosystem of linking the government, the CCP, the economy, and, occasionally, the military. Analysts have termed China's approach to fusing these sectors as "state capitalism."[192] There are different arguments as to why the PRC's kind of state capitalism is problematic from the perspective of emergent economies (or liberal democracies, for that matter).[193]

The first is companies' ownership structure. There has been much debate about the ownership of Chinese companies, in terms of how or whether Chinese state interests influence the design and operation of the companies' equipment to facilitate state-

---

[190] Li-Wen Lin & Curtis J. Milhaupt, *We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China*, 65 STAN. L. REV. 697 (2013); CHING KWAN LEE, THE SPECTER OF GLOBAL CHINA: POLITICS, LABOR, AND FOREIGN INVESTMENT IN AFRICA 32 (2018) (finding that central SOEs are motivated not only by profit but also by the "nation's strategic, lifeline, security interests").

[191] *See e.g.*, U.S. Department of Justice, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," (Feb. 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering (detailing how a superseding indictment was handed down in federal court in Brooklyn, New York, charging Huawei with violating the Racketeer Influenced and Corrupt Organizations Act) and U.S. Department of Commerce, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies," (May 15, 2020), https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts (restricting Huawei's ability to use U.S. technology and software to design and manufacture its semiconductors abroad because "Huawei is engaged in activities that are contrary to U.S. national security or foreign policy interests.")

[192] *See* Lin & Milhaupt *supra* note 190 at 706-7; BARRY NAUGHTON & KELLEE S. TSAI, STATE CAPITALISM, INSTITUTIONAL ADAPTATION, AND THE CHINESE MIRACLE (2015); Benjamin L. Liebman & Curtis J. Milhaupt, REGULATING THE VISIBLE HAND? THE INSTITUTIONAL IMPLICATIONS OF CHINESE STATE CAPITALISM (2016); *contrast* BRANKO MILANOVIC, CAPITALISM, ALONE: THE FUTURE OF THE SYSTEM THAT RULES THE WORLD 87–96 (2019) (describing China's system as "political capitalism" with efficient bureaucracy, absence of rule of law, and autonomy of the state).

[193] *See also* Mark Wu, *The "China, Inc." Challenge to Global Trade Governance*, 57 HARV. J. INTL. L. 261 (2016) (analyzing why the rise of China presents a challenge to the WTO's multilateral trade regime).

directed intelligence gathering and covert cyber operations.[194] The MNCs, most prominently Huawei and ZTE, are nominally wholly owned by their employees but critics have pointed out that their ownership structure is more complicated than their self-representation would suggest. For instance, Huawei is owned by a holding company, which is, in turn, is approximately 1 percent owned by the Huawei founder Ren Zhengfei and 99 percent owned by a "trade union committee."[195] Members of the trade union committee, critics point out, do not own stock in Huawei or its holding company, rather, they have a kind of "virtual stock" through contract that allows them to share in profits.[196] As a contract right, rather than a property right, the virtual stock provides no basis for voting power and hence no control over the company. Huawei's "virtual stock" may not differ too much from ownership models familiar to startups in Silicon Valley.[197] However, there are important differences. Trade unions in China operate under the control of the CCP and have traditionally functioned to fulfill state and CCP directives.[198]

The second argument concerns state capture.[199] Intelligence gathering for national security purposes is particularly prominent in the debate. The common example recycled in the U.S. media is the legal requirement that Chinese companies submit data to the PRC government upon request. The basis for this command is the National Intelligence Law of 2018 and the Counter-Espionage Law of 2014.[200] Yet state capture may also operate outside of legal requirements. These mechanisms of state capture include politically connected entrepreneurs, governmental subsidies, and extralegal control through, for example, chambers of commerce, which coordinate activities within an industry to align them with the party-state's interests.[201] The requirement that all companies in China—domestic and foreign-invested—have a party cell is written into PRC law.[202] The CCP has focused on embedding itself within technology firms, in particular. Huawei, for

---

[194] U.S. House of Representatives, Permanent Select Committee on Intelligence, *Investigation of the Security Threat Posed by Chinese Telecommunications Companies Huawei and ZTE* (Sept. 13, 2012), https://www.hsdl.org/?view&did=722516.

[195] Balding, Christopher and Clarke, Donald C., *Who Owns Huawei?* (April 17, 2019), available at SSRN: https://ssrn.com/abstract=3372669.

[196] *Id*.

[197] *See e.g.*, Alex Lazarow, *Beyond Silicon Valley*, HARV. BUS. REV. (March-April 2020), https://hbr.org/2020/03/beyond-silicon-valley (describing the example of Fenix International, whereby the CEO created phantom shares called "Fenix Flames," which resembled direct stock ownership, to provide equity incentives for employees).

[198] CYNTHIA ESTLUND, A NEW DEAL FOR CHINA'S WORKERS? 190 (2017).

[199] Curtis J. Milhaupt & Wentong Zheng, *Beyond Ownership: State Capitalism and the Chinese Firm*, 103 GEORGETOWN L. J. 665 (2015).

[200] Zhonghua renmin gongheguo guojia qingbaofa (中华人民共和国国家情报法) [National Intelligence Law of the PRC], promulgated by the NPC on Apr. 27, 2018 and effective on Apr. 27, 2018, art. 7 (requiring that any organization or citizen shall support national intelligence work) and Zhonghua renmin gongheguo fanjiandiefa (中华人民共和国反间谍发) [Counterespionage Law of the PRC], promulgated by the NPC on Nov. 1, 2014 and effective on Nov. 1, 2014, art. 22 (mandating that organizations shall provide information or evidence to a national security authority when requested to do so).

[201] Milhaupt & Zheng *supra* note 199 at 683-6.

[202] *See* Zhonghua renmin gongheguo gongsi fa (中华人民共和国公司法) [PRC Company Law], promulgated by the NPC on Oct. 26, 2018 and effective Oct. 26, 2018, art. 19 (requiring companies to provide the "necessary conditions" to facilitate the activities of party organizations).

instance, has 300 party branches, Alibaba 200, and Tencent 89.[203] For these reasons, it is impossible to disentangle Chinese tech companies' operations from the interests of the party-state.

Chinese technology companies are also engaged in institution building in the context of the DSR. Alibaba and the Hangzhou government jointly established an eWTP in Hangzhou, and in 2017, Malaysia and Alibaba jointly launched the first eWTP "experimental zone," the Malaysian Digital Free Trade Zone, outside China.[204] The two hubs are interconnected to promote cooperation in customs clearance, inspection and licensing, and explore data-driven trade facilitation and policy innovation.[205] The WTO and the World Economic Forum (WEF) have been supportive of the eWTP as a complement to their institutional infrastructure in favor of economic globalization, in one example of China's openness to cooperating with international organizations.[206] Based on Hangzhou's approach to a "cashless society," Ant Financial, an affiliate of Alibaba which operates Alipay, the largest online payments platform in the world, has extended such digital financial transaction infrastructure to Singapore, Thailand, the Philippines, Vietnam, and most recently, to Malaysia. In Malaysia, under cooperative agreements, two central Malaysian banks have accepted Alipay allowing up to 80 percent of merchants in Malaysia to use the platform.[207]

Meanwhile, Chinese telecommunication companies have expanded their global reach through the DSR. The telecom industry in China is run by three SOEs: China Mobile, China Unicom, and China Telecom. These SOEs have each established a global presence, in line with BRI trajectories, by entering emerging markets through either acquiring shares in domestic companies[208] or forming consortia.[209] As a result, China

---

[203] *See* Cave et al., *supra* note 15 at 7.

[204] Anon. Alibaba eWTP shouge haiwai 3-hub zai Malaixiya zhengshi qudong (阿里巴巴 eWTP 首个海外 e-hub 在马来西亚正式启动) [Alibab's eWTP's First Overseas E-Hub Officially Launched in Malaysia] Alibaba jituan (阿里巴巴集团) [Alibaba Group] (Nov. 3, 2017), https://www.alibabagroup.com/cn/news/article?news=p171103.

[205] Anon. Alibaba datong zhongma "shuzi zhongshu" jiakuai tuijin eWTP (阿里巴巴打通中马"数字中枢" 加快推进 eWTP) [Alibaba Opens up China-Malaysia "Digital Hub" and Accelerates eWTP] Alibaba jituan (阿里巴巴集团) [Alibaba Group] (May 12, 2017), http://www.sohu.com/a/140036056_270234.

[206] WTo-eWTP-WEF Enabling E-Commerce Launch Event, WORLD TRADE ORGANIZATION (Dec. 11, 2017), https://www.wto.org/english/news_e/spra_e/spra206_e.htm (detailing remarks by the Director General of the WTO regarding cooperation with Jack Ma, founder of Alibaba).

[207] Anon. Mayi jinfu qianzhou Malaixiya yinhang 8cheng shangdianhu dou neng shiyong Zhifubao (蚂蚁金服牵手马来西亚银行 8 成商户都能使用支付宝) [Ant Financial Partners with Bank of Malaysia, 80% of Merchants Can Use Alipay] Jinrongjie wangzhan (金融界网站) [Finance World Net] (Mar. 23, 2017), http://bank.jrj.com.cn/2017/03/23182822219003.shtml.

[208] Anon. *China Mobile Acquires Paktel*, DAWN (May 19, 2007), https://www.dawn.com/news/247615 (China Mobile acquired 88.86 percent interest in Paktel Ltd., the first cellular operator in Pakistan, for $460 million). *See also* Zhongguo yidong quanqiu buju? Bushi mai lege jingwai qiye, jiu jiao "quanqiu buju" (中国移动全球布局？不是买了个境外企业，就叫"全球布局") [China Mobile's Global Distribution? Instead of Buying an Overseas Company, it's Called "Global Distribution."], Sohu (May 28, 2017), http://www.sohu.com/a/137090323_465600 (describing how China Mobile acquired minority stakes in Thai telecom operator True, and in Axiata, Malaysia's largest wireless carrier).

Unicom International Ethernet Private Line is available in 50 major countries and regions.[210] China Unicom has also built an interconnected cloud platform that allows users to use any China Unicom cloud node to access globally-distributed public clouds.[211] Further, China Unicom has opened international roaming 4G services covering 112 countries and regions and established ten overseas wholly-owned subsidiaries and 21 offices overseas.[212] In 2017, China Unicom set up branches in eleven countries along the BRI including Russia, Indonesia, Malaysia, Vietnam, Thailand, Myanmar, India, Kazakhstan, United Arab Emirates, the Philippines and South Africa.[213] In all, investment in BRI states accounted for 82 percent of China Unicom's foreign investments in 2017.[214]

MNCs like Huawei and ZTE are strong backers of the DSR. These companies are the main drivers behind China's export of surveillance technology.[215] China is supplying surveillance technology to 63 countries, 36 of which are BRI members.[216] Huawei is the lead supplier of such technology in the world, providing surveillance equipment to over 50 countries worldwide.[217] ZTE has a permanent presence in 53 BRI states, wireless networks covering 40 countries, and wired networks covering 52 countries.[218] ZTE has assisted the construction of a communication network for the DSR in three ways: one, building cross-border network interconnections, two, accelerating national networks, and, three, facilitating service interoperability.[219] There are a number of ways that ZTE achieves these aims: first, ZTE works with the three telecom SOEs to speed up cross-border interoperability.[220] Second, ZTE has constructed both wireless and wire-line communication networks for BRI member states, including, Pakistan, Indonesia, Vietnam, Thailand, and Turkey.[221] Third, ZTE helps build data centers and other services for BRI states and the MNCs that operate in those jurisdictions. For example, ZTE

---

[209] Ma Si, *China Telecom Enters Philippine Market*, CHINA DAILY (Nov. 21, 2018), http://global.chinadaily.com.cn/a/201811/21/WS5bf4ad00a310eff303289fe2.html (China Telecom formed Mislatel consortium to enter the Philippines market).
[210] China Unicom, IEPL, https://www.chinaunicomglobal.com/au/iepl (last visited Aug. 17, 2020).
[211] China Unicom, Public Clouds, https://www.chinaunicomglobal.com/hk/sci. (last visited Apr. 4, 2020).
[212] Wu Weiqun (吴卫群), Zhongguo liantong jinnian ni touzi jingwai xiangmu, "yidaiyilu" quyu zhan bida 82% (中国联通今年拟投资的境外项目，"一带一路"区域占比达 82%) [In the Overseas Projects China Unicom Intends to Invest In this Year, the "Belt and Road" Initiative Accounts for 82%], Shangguan (上观) [Shanghai Observer] (Aug. 17, 2020), https://www.jfdaily.com/news/detail?id=52988.
[213] *Id*.
[214] *Id*.
[215] Steven Feldstein, *The Global Expansion of AI Surveillance*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (Sept. 2019), 16, https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final.pdf. (clarifying that the export of "AI surveillance" technology is common across liberal and authoritarian countries).
[216] *Id*. at 1.
[217] *Id*. at 1, 13.
[218] Anon. Zhongxing Tongxun Zhao Xianming: jianzhe "yidaiyilu" guojia xinxi gaosu gonglu (中兴通讯赵先明：建设"一带一路"国家信息高速公路) [ZTE Zhao Xianming: Building "Belt and Road" National Information Highway] Sina (May 22, 2017), https://tech.sina.com.cn/roll/2017-05-22/doc-ifyfkqwe0661865.shtml.
[219] *Id*.
[220] *Id*.
[221] *Id*.

invested more than $100 million in the Bangladesh National Data Center.[222] In these ways, the private sector complements state-directed activity in building the DSR.

In addition to these core telecommunication infrastructures, Chinese technology companies increasingly provide personal telecommunications services in form of social media platforms. In China, Tencent's WeChat has become the dominant social network with approximately one billion users per day.[223] WeChat's users outside of China are still relatively small, at about 100-200 million active users per month.[224] The Chinese diaspora in Southeast Asia has promoted the use of the network in places like Malaysia, where there are some 20 million users and Thailand, where approximately 17 percent of the population uses the app.[225] TikTok has garnered an even broader user base outside of China than WeChat. TikTok merged with the U.S. app Musical.ly in August 2018 and was fined by the U.S. Federal Trade Commission in 2019 for illegally collecting information about users under thirteen.[226] In Indonesia, TikTok was temporarily banned for displaying "pornography, inappropriate content and blasphemy."[227] Like their Western counterparts, Chinese social media platform face an increasingly complicated landscape of governmentally mandated content moderation, thereby complicating their efforts to have a globally uniform product outside China in addition to the Chinese version, which has to comply with the PRC's complex censorship regime.

Chinese technology companies are investing heavily into research and development (R&D), which may be consequential for the future design and configuration of digital infrastructures. Huawei, for example, invests 10 percent of its sale revenue annually in R&D.[228] BRI countries have been essential to Huawei's growth, where, in its formative years, some 70% of its markets were outside of China, in neighboring Asian countries and Africa, commensurate with today's BRI.[229] Huawei's R&D investments in these countries reflect their proportion of the company's portfolio as Huawei looks to the

---

[222] *Id*.
[223] Mansoor Iqbal, *WeChat Revenue and Usage Statistics (2020)*, BUSINESS OF APPS (Jul. 30, 2020), https://www.businessofapps.com/data/wechat-statistics/.
[224] *See* Cave et al. supra note 15.
[225] *Id*.
[226] Federal Trade Commission, *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That is Violated Children's Privacy Law* (Feb. 27, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.
[227] Anon. *Indonesia Bans Chinese Video App Tik Tok for 'Inappropriate Content'*, REUTERS (Jul 4, 2018), https://www.reuters.com/article/us-indonesia-bytedance-ban/indonesia-bans-chinese-video-app-tik-tok-for-inappropriate-content-idUSKBN1JU0K8.
[228] Anon. "Yidaiyilu" yanxian diaoyan | Huawei zai e ershinian: Zhongguo qiye ruhe zhagen haiwai ("一带一路"沿线调研 | 华为在俄二十年:中国企业如何扎根海外) ["Belt and Road" Research and Development: Huawei's Twenty Years in Russia: How do Chinese Companies Take Root Overseas] Sohu (Sept. 5, 2018), https://www.sohu.com/a/252139057_661660.
[229]Anon., Zhang Yansheng: Huawei you jintian quan kao 'yidaiyilu'" (张燕生：华为有今天全靠"一带一路") [Zhang Yansheng: Huawei Today Entirely Depends on the 'Belt and Road'], (Nov. 30, 2017), Xinlang caijing (新浪财经) [Sina Finance], http://finance.sina.com.cn/meeting/2017-11-30/doc-ifyphxwa7115289.shtml.

BRI countries to establish its own intellectual property rights, brand, and market channels.[230]

C. The DSR's Legal and Institutional Governance Infrastructure

China has valorized the WTO as the fundamental infrastructure of the global economic order and relies on additional free trade and bilateral investment agreements with BRI countries. There is no comparable legal infrastructure in place for the DSR as China does not promote its approach to data governance through trade agreements and refrains from signing on to the models that the EU and U.S. are promoting.[231] In lieu of treaties under international law, the PRC has established non-binding bilateral and multilateral instruments for international coordination between itself and DSR host states. As of 2019, China signed cooperative agreements with some sixteen countries to promote the DSR.[232]

One programmatic statement of the DSR is the "Belt and Road Digital Economy International Cooperation Initiative" (*Yidaiyilu shuzi jingji guoji hezuo changyi*, hereinafter, "the Digital Initiative"), launched by China and six other BRI countries in December 2018.[233] The Digital Initiative is comprised of fifteen general principles to "strengthen policy communication, connectivity, trade, financing, and popular sentiment." Some principles refer directly to physical components of digital infrastructure ("expand broadband access and improve broadband quality"). Others are concerned with developing a digital economy generally ("promote digital transformation," "promote development of small, medium, and micro enterprises"), sectorally ("promote e-commerce cooperation", "promote investment in the field of information and communication technology"), but also societally ("strengthen digital skills training"; "improve digital inclusion"; "strengthen confidence and trust").

"Full respect" for cyber sovereignty is explicitly mentioned in principle 14, which encourages the construction of "peaceful, safe, open, cooperative, and orderly cyberspace." The principle implicitly acknowledges the inherent tension between the "openness" that is facilitated through enhanced digital connectivity and governmental control over data flows. The same principle also calls for the "establishment of a multilateral, democratic, and transparent international Internet governance system," echoing the long standing debate about erstwhile U.S.-dominated multi-stakeholder

---

[230] *Id*.

[231] *See supra* §II.C.

[232] Tuijin "yidaiyilu" jianshe gongzuo lingdao xiaozu bangongshi (推进"一带一路"建设工作领导小组办公室) [Office of the Leading Small Group for Promoting the Work of Constructing the "Belt and Road Initiative"], Gongjian "yidaiyilu" changyi: jinzhan, gongxian yu zhanwang (共建"一带一路"倡议：进展、贡献与展望) [Jointly Sponsor the "Belt and Road Initiative": Progress, Contribution, and Prospects] (2019), http://www.xinhuanet.com/world/2019-04/22/c_1124400071.htm.

[233] The other countries are Laos, Saudi Arabia, Serbia, Thailand, Turkey, and the UAE. *See* Anon. "Yidai yilu" shuzi jingji guoji hezuo changyi) 《"一带一路"数字经济国际合作倡议》发布) [Launch of the "Belt and Road" Digital Economy International Cooperation Initiative] (May 11, 2018), http://www.cac.gov.cn/2018-05/11/c_1122775756.htm.

Internet governance institutions, such as ICANN, against which China has consistently argued for more governmental control over the Internet within rather than outside the UN framework.[234] Similarly, principle 13, "to encourage cooperation and respect for independent development," seeks to reconcile the inevitable dynamic of "cooperating" in a highly uneven relationship with a digital super-power with DSR host states' interest in charting their own path into a digital future. This language differs markedly from the ways in which the U.S. and EU have been promoting their respective models for digital development.[235]

Three principles of the Digital Initiative address governance issues explicitly. Firstly, the document encourages "the development of transparent digital economic policies." A closer look at this transparency principle reveals that the type of transparency called for is connected to the "e-government" strategy China has promoted in recent decades (and Singapore has perfected) with a focus on open tendering and procurement.[236] In this conception of "transparency," censorship of political speech is not anathema to commercial transparency. Secondly, the Digital Initiative calls for the promotion of international standards. Against a common assumption that the BRI is trying to displace existing international organizations, in practice, the BRI, including the DSR, operates, in many cases, through existing platforms for international cooperation.[237] Indeed, where applicable and helpful, the Chinese government has sought to build the DSR into existing international regulatory frameworks.[238] For instance, in 2017, the PRC Ministry of Industry and Information Technology (MIIT) signed a letter of intent with the ITU, to coordinate Information and Communication Technologies (ICTs) in the context of the BRI and, in 2019, the Export-Import Bank of China signed an MOU for promoting the 2030 Agenda for Sustainable Development through the BRI with the ITU.[239] As most BRI states are members of the WTO, technology products and services are to be "consistent with international rules, including WTO rules and principles."[240] Thirdly, the Digital Initiative encourages the establishment of multi-level communication mechanisms among governments, businesses, scientific research institutions, and industry organizations. The principle calls explicitly for the exchange of "policy formulation and legislative experience" and to "share best practices" among countries along the BRI. These exchanges may contribute to the "Beijing Effect."[241]

---

[234] *See supra* §II.C.
[235] *See supra* §II.C.
[236] Ian Holiday, *Building E-Government in East and Southeast Asia: Regional Rhetoric and National (In)Action*, 22 PUBLIC ADMIN. & DEV. 323 (2002).
[237] *See supra* text accompanying note 136.
[238] *See e.g.*, Anon. Ershi guo jituan shuzi jingji fazhan yu hezuo changyi (二十国集团数字经济发展与合作倡议) [The G20 Digital Economy Development and Cooperation Initiative] (Sep. 9, 2016), http://www.cac.gov.cn/2016-09/29/c_1119648520.htm. On China's leadership in building international investment standards in the G20, *see* Karl P. Sauvant, *China Moves the G20 towards in International Investment Framework and Investment Facilitation*, *in* CHINA'S INTERNATIONAL INVESTMENT STRATEGY: BILATERAL, REGIONAL, AND GLOBAL LAW AND POLICY 311 (Julien Chaisse ed. 2019).
[239] Sen Gong et al, *supra* note 15; *see also* Ministry of Foreign Affairs of China, List of Deliverables of the Second Belt and Road Forum for International Cooperation (Apr. 27, 2019), http://www.globaltimes.cn/content/1147744.shtml.
[240] Digital Initiative, *supra* note 233.
[241] *See supra* §II.C.

In addition to the Digital Initiative and reflecting the hub and spoke nature of the BRI, China, through the MIIT, has also signed MOUs with government agencies in Cambodia, Iran, Bangladesh, and Afghanistan.[242] It has further signed agreements with the five member states of the East African Community, Ethiopia, and the ITU to build "information highways" (not to be confused with those touted by Al Gore thirty years ago) in East Africa.[243] Regionally, it has issued an action plan to partner with ASEAN to develop ICTs.[244] Similarly, Chinese MNCs have also established soft law agreements with foreign governments to support the DSR. Most of the initiatives discussed above, namely, the data centers and cloud networks are a result of such agreements. For example, Alibaba signed an MOU with the Thai government in April 2018 to establish an AI data center in the Eastern Economic Corridor to assist the digitization of SMEs located there and to enhance e-commerce.[245]

All these arrangements provide a general framework for coordination along the DSR without mandating a certain approach to data governance. However, as argued above, BRI or DSR states may replicate certain elements China's approach to data governance because it accords with their policy preferences. For instance, an MOU between China and Hungary was formed concurrently with a new Digital Government Agency in Hungary, in charge of IT procurement and controlled by Fidesz, the ruling party.[246] While ostensibly providing transnational connectivity through Chinese SOEs and private companies, the DSR might lead to domestic data enclosures, if host states decide to mimic China's domestic data governance regime and create data control infrastructures comparable to China's. In this way, the Chinese party-state may influence both legal and infrastructural data governance in BRI states.

IV. A Digital Silk Road Case Study: Pakistan

In this section, we focus on Pakistan to illustrate the DSR-induced Beijing Effect in a developing country. We chose Pakistan due to the significance of the Sino-Pakistani relationship, the prominence of the China-Pakistan Economic Corridor (CPEC) within the BRI, and the country's hedging strategy, which is characteristic of many developing economies.[247] The *Long Term Plan for China-Pakistan Economic Corridor (2017-2030)* (hereinafter, *Long Term Plan*) defines CPEC as "a growth axis and a development belt" linking China and Pakistan encompassing a "comprehensive transportation corridor and

[242] Sen Gong et al., *supra* note 15, at 5.
[243] *Id.*
[244] *Id.*
[245] *Id.*
[246] Bilateral Action Plan on Digital Silk Road Cooperation, signed by the National Development and Reform Commission and the Ministry of Innovation and Technology of Hungary, during the Second Belt and Road Forum for International Cooperation in Beijing on Apr. 27, 2019. *See* http://www.globaltimes.cn/content/1147744.shtml. Contrary to the "transparency principle" of the Digital Initiative, this document has not been made public.
[247] Trang (Mae) Nguyen, *International Law as Hedging: Perspectives from Secondary Authoritarian States*, 144 AJIL UNBOUND 237, 237-8 (2020) (explaining how small states use international law to "hedge" major powers).

industrial cooperation…with concrete economic and trade cooperation, and people-to-people exchange and cultural communication" aimed at major collaborative projects for infrastructure construction, industrial development and livelihood improvement."[248] The DSR is also a foundational part of CPEC; the *Long Term Plan* identifies "information network infrastructure" as one of the key areas for cooperation.[249] In the following, we analyze the impact of the DSR on Pakistan with reference to digital connectivity, surveillance infrastructures in "safe" cities, and its evolving domestic data governance regime.

A. Digital Connectivity within Pakistan and Beyond

While much of the popular press in Pakistan, China, and elsewhere has focused on CPEC's major energy projects and mass transit systems, CPEC also shows the primacy of data flows in China's cross-border development. The *Long Term Plan* identifies the following specific items for "information network infrastructure":

1. Promote the construction of cross-border optical fiber cables between China and Pakistan and the construction of the backbone optical fiber networks in Pakistan.
2. Upgrade Pakistan's network facilities, including the national data center and the second submarine cable landing station.
3. Expedite Pakistan to adopt China's Digital Terrestrial Multimedia Broadcasting (DTMB) standard.
4. Promote the ICT-enabled development of Pakistan, including e-government, border electronic monitoring and safe city construction; promote the development of e-commerce in Pakistan.
5. Enhance the development of the information industry in Pakistan; build IT industrial parks and IT industry clusters in Pakistan to improve Pakistan's information technology and service outsourcing.
6. Increase Pakistani personnel in exchange programs in China, establish technical training centers in Pakistan, and strengthen the construction of ICT human resources in Pakistan.[250]

These goals broadly reflect patterns of China's approach to transnational data governance outlined above, including supplying digital infrastructures like fiber optic cables and data

[248] GOVERNMENT OF PAKISTAN MINISTRY OF PLANNING, DEVELOPMENT AND REFORM AND THE PEOPLE'S REPUBLIC OF CHINA NATIONAL DEVELOPMENT & REFORM COMMISSION, LONG TERM PLAN FOR CHINA-PAKISTAN ECONOMIC CORRIDOR 4 (2017-2030) (on file with the authors). There is some controversy about this document. Journalists had obtained copies of a much longer "Long Term Plan" (dated December 2015) but officials made public a shorter version in February 2017. There is debate as to whether they are different drafts of the same document or different documents, one "internal" and the other a sanitized version for public consumption. For an assessment of the longer version *see* Khurram Husain, *Exclusive: CPEC Master Plan Revealed*, DAWN (Jun. 21, 2017), https://www.dawn.com/news/1333101.

[249] *Id.*

[250] *See* Long Term Plan *supra* note 248, at 15.

centers, setting technical standards, and promoting the growth of digital economies abroad in connection to China.[251]

Pakistan and the broader South Asian region, including India, are alluring markets for Chinese technology companies. Pakistan has a population of 212 million, most of it young and quickly urbanizing. According to one report, Pakistan is one of five countries that will account for 50% of the growth of 1.6 billion new mobile Internet users by 2025.[252] At the same time, Huawei's Global Connectivity Index ranked Pakistan 77 out of 79 countries in the world for ICT.[253] Putting Pakistan's growth potential together with its existing poor digital infrastructure, Chinese tech companies are particularly keen to gain a foothold in the country and Pakistani promoters of e-commerce are generally supportive.[254]

Considerable strides have been made to connect China to Pakistan through digital infrastructures.[255] In 2018, the Pakistan-China Fiber Optic Project was finalized, connecting Pakistan and India through a new terrestrial fiber-optic cable between the Khunjerab Pass on the China-Pakistan border and the city of Rawalpindi.[256] The cable connects Pakistan to the Transit Europe-Asia Terrestrial Cable Network, thereby reducing Pakistan's dependence on submarine cables for transnational connectivity. In addition, construction of a new Pakistan East Africa Cable Express (PEACE), a submarine cable system, purported to be the most direct route for high-speed Internet traffic between Africa and Asia is currently underway with landing points in Gwadar and Karachi.[257]

Pakistan's emergent data links to China are not just over or below the ground, but also through space. Pakistan was one of the first adopters of the BeiDou Navigation Satellite System (*Beidou weixing daohang xitong*), which is billed as a rival to GPS (the globally dominant U.S. system), Galileo (the EU alternative under construction), and

---

[251] *See supra* §II.

[252] BYTES FOR ALL, PAKISTAN'S INTERNET LANDSCAPE 2018 11 (2018), https://bytesforall.pk/publication/pakistans-internet-landscape-2018 (citing a report by GSMA Intelligence).

[253] *Id.*

[254] *Id.* at 79 (quoting Syed Salman Hassan, CEO TCS Ecom, as saying "The potential of the Pakistani consumers—200 million plus population with 65pc below the age of 30—is finally being realized. With Alibaba entering in the local market, it will get better from here onwards. Jack Ma and Alibaba have been supportive of the small-and medium-enterprises sector and China is proof.").

[255] *But see* Jonathan E. Hillman and Maesea McCalpin, *The China-Pakistan Economic Corridor at Five*, CENTER FOR STRATEGIC & INT'L STUDIES BRIEFS (Apr. 2, 2020), https://www.csis.org/analysis/china-pakistan-economic-corridor-five (observing "mixed implementation" among CPEC's eight ICT projects).

[256] Zafar Bhutta, *Pak-China Fibre Optic Cable to Start Functioning by Year-End*, THE EXPRESS TRIBUNE (Sep. 16, 2018), https://tribune.com.pk/story/1804386/2-pak-china-fibre-optic-cable-start-functioning-year-end/.

[257] Jonathan E. Hillman, *War and PEACE on China's Digital Silk Road*, CENTER FOR STRATEGIC AND INT'L STUDIES (May 16, 2019), https://www.csis.org/analysis/war-and-peace-chinas-digital-silk-road; https://www.submarinenetworks.com/en/systems/asia-europe-africa/peace/pakistan-to-be-linked-with-peace-cable-system-with-up-to-60tbps-capacity.

GLONASS (the Russian system).[258] Originally developed by the Chinese military in the early 2000s to avoid reliance on GPS, BeiDou has since gained commercial traction and PRC phones made by Huawei, Xiaomi, and others are all BeiDou-compatible. BeiDou achieved global coverage in June 2020.[259] Some have suggested that Pakistan's military may have access to the high precision military signal that is otherwise reserved for China's armed forces.[260]

Whereas Chinese technology companies have made major inroads into Asia more generally,[261] perhaps nowhere is their presence more felt than in Pakistan. In the telecommunications industry, China Mobile entered Pakistan's market in 2009 and in that period has created a digital ecosystem and evolved Pakistani mobile-phone users through 2G to 4G technologies with plans for systems to be upgraded to 5G during 2020. Zong 4G, the local brand for China Mobile Pakistan, has surpassed its competitors in terms of market share with over 32 million subscribers, 18 million broadband subscribers, over 10 million 4G subscribers, and through having built 10,550 base stations with 4G services across the country.[262] While the U.S. and some of its allies scorn Huawei, Pakistan is embracing the company. Zong 4G and Huawei announced in early 2019 that they would partner to optimize their networks.[263] Huawei Marine, a subsidiary of Huawei, is also involved in building the PEACE project, mentioned above.[264]

In addition to mobile technology, Chinese companies have established a strong presence in data finance and e-commerce in Pakistan. Pursuant to the logic of state capitalism, the heads of the respective two governments have had a "visible hand" in linking Chinese e-commerce to that of Pakistan. After the first BRI Forum in Beijing, then-Prime Minister Sharif visited the headquarters of Alibaba Group in Hangzhou and on the same day, the Pakistan Trade Development Authority and Alibaba signed an MOU to promote the globalization of Pakistan's SMEs through e-commerce.[265] As part of the

---

[258] Degan Sun and Yuyou Zhang, *Building an "Outer Space Silk Road": China's Beidou Navigation Satellite System in the Arab World*, 10 J. OF MIDDLE EASTERN AND ISLAMIC STUDIES (IN ASIA) 24 (2018).
[259] Anon., *BeiDou: China launches final satellite in challenge to GPS*, BBC (Jun 23, 2020), https://www.bbc.com/news/business-53132957.
[260] Anon., *Pakistan Becomes One of the First Country to Hook on to China's BeiDou Satellite Navigation System for Military Purpose: Sources*, TIMES OF ISLAMABAD (Jan. 2, 2019), https://timesofislamabad.com/02-Jan-2019/pakistan-becomes-one-of-the-first-country-to-hook-on-to-china-s-beidou-satellite-navigation-system-for-military-purpose-sources.
[261] Brian Harding, *China's Digital Silk Road and Southeast Asia*, CENTER FOR STRATEGIC AND INT'L STUDIES (Feb. 15, 2019), https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia.
[262] Xinhua, *Chinese Enterprise Plays Pivotal Role in Promoting Pakistan's Telecom Infrastructure: Minister*, CHINA DAILY (Jan. 30, 2019), http://www.chinadaily.com.cn/a/201901/30/WS5c513825a3106c65c34e7543.html.
[263] Muhammad Hamza, *Zong 4G and Huawei Partner for Digital Transformation*, TECHWIRE (Feb. 7, 2019), https://www.technologytimes.pk/zong-4g-huawei-digital-transformation/.
[264] Winston Qiou, *Pakistan to be Linked with PEACE Cable System with up to 60Tbps Capacity*, SUBMARINE CABLE NETWORKS (Apr. 16, 2018), https://www.submarinenetworks.com/en/systems/asia-europe-africa/peace/pakistan-to-be-linked-with-peace-cable-system-with-up-to-60tbps-capacity.
[265] Anon., *Alibaba Signs MoU with Trade Development Authority of Pakistani to Support E-commerce Development of SMEs and Financial Services*, ALIBABA GROUP (May 16, 2017), https://www.alibabagroup.com/en/news/article?news=p170516.

deal, Chinese companies were to help build Pakistan's e-commerce infrastructure.[266] Subsequent to this agreement, Ant Financial acquired a 45 percent stake in Telenor Microfinance Bank, based in Karachi, from Telenor, a Norwegian telecommunications company.[267] Two months later, Alibaba acquired 100 percent shares in Daraz, Pakistan's top online retailer, incubated by Germany's Rocket Internet.[268] Major acquisitions in both fintech and e-commerce is a common strategy of Alibaba in Asia, although other countries like India have been more protective of such industries than Pakistan. While Chinese acquisitions provide greater and cheaper access to mobile phones and telecommunication services, greatly increasing the penetration of the Internet into the country, Pakistani experts cited a number of concerns, ranging from corporate governance and lack of anti-corruption enforcement to cybersecurity and surveillance risks, concerns which are apropos given Pakistan's nascent legislation.[269]

In the impression of one interlocutor, in contrast to European and American companies, which are known to be relatively stringent in following local law, Chinese companies have a more adaptive approach.[270] Pakistani industry insiders have stated that Chinese companies obtain privileged information from the chamber of commerce, and with this information, they built a platform through which Pakistani vendors compete with each other. In this process, Chinese companies have been known to receive illicit payments, a practice which appears generally tolerated by local authorities.[271] Although we are aware of the danger of extrapolating from anecdotal accounts to make broad statements about the corporate culture of Chinese technology companies, it seems safe to say that companies may emphasize corporate compliance only to the extent that the host state effectively demands it. Relevant Pakistani regulatory agencies, for example, the newly reformed Pakistan Media Regulatory Authority, which now includes "cyber media," may emphasize state control over transparent rules, thus creating an environment for the growth of cross-border para-statal corporations.[272]

B. Chinese Surveillance Infrastructure in "Smart" and "Safe" Cities

The most striking implication for the spread of the DSR into Pakistan may be surveillance, in particular in form of "smart" or "safe" cities, as they are more commonly known in Pakistan. China is leading the world in the promotion of "smart cities" that use big data analytics for urban governance.[273] Huawei alone has supplied 75 "smart city-

---

[266] *Id.*
[267] Shahbaz Rana, *CCP Approves Alipay's 45% Stake in Telenor Microfinance Bank*, THE EXPRESS TRIBUNE (Nov. 8, 2018), *available at* https://tribune.com.pk/story/1842703/2-ccp-approves-alipays-45-stake-telenor-microfinance-bank/.
[268] Sumaira Jajja, *As Alibaba buys Daraz, Many Ask: What Next?*, DAWN (May 9, 2018), https://www.dawn.com/news/1406501.
[269] *See infra* §IV.C.
[270] Interview, Islamabad, Apr. 2, 2019.
[271] *Id.*
[272] *But see infra* text accompanying note 321.
[273] *See generally* Alan Smart, *The Prospects and Social Impact of Big Data-Driven Urban Governance in China: Provincializing Smart City Research*, *in* CHINA URBANIZING: IMPACTS AND TRANSITIONS (Weiping Wu & Qi Gao eds., In Press).

public security projects" globally.[274] Digital technologies can facilitate public services but the tradeoffs are obvious. Facial recognition technologies strengthen the surveillance capabilities of governments and may violate equal protection, privacy, and consumer rights.[275]

"Safe cities" are particularly attractive to Pakistan given its concerns for public order. Starting in 2015, a number of sub-national police authorities were established, such as the Punjab Safe Cities Authority (PSCA), to build "safe" cities.[276] Chinese technology is highly attractive to regulators such as the PSCA for its integrated solutions to problems of urban governance.[277] Early on, Huawei became the implementing partner to the PSCA to supply equipment to a number of "safe" cities in Punjab. The Lahore Safe City project, for instance, under the PSCA, features a command and control center for an area of over 76,000 square feet by using cloud and other ICT technologies, and some 10,000 surveillance cameras designed and installed by Huawei.[278] Huawei was awarded the contract in 2016 for a total of $84.7 million.[279] At the time, Huawei touted the project as "the largest comprehensive Safe City architecture in the world."[280] The project became controversial, however, when it was discovered that the system's CCTV cabinets included undisclosed WiFi transmitters, raising questions about data security.[281]

Members of civil society also report that the technology provided by Huawei has allowed the PSCA to remove what they deem to be objectionable material from the Internet within their "safe cities," an act that exceeds their official mandate.[282] Further complicating the picture, while "safe city" technology was originally designed for police use and for traffic control, the Pakistani military and intelligence services have since operationalized these networks. The union of Pakistani law and security enforcement with Chinese digital infrastructure shows both the benefits and pitfalls of mutual access. Whereas the technology may strengthen the police powers of local and national authorities, it may do so in ways that may exceed the relevant laws. Meanwhile, whereas

---

[274] *See* Cave et al. *supra* note 15 at 10.

[275] *See e.g.*, Zhejiang Pufa (浙江普法) [Zhejiang Law Popularization], Yin dongwu shijie qiyong renlian shibie, Zhejiang yi daxue jiaoshou jiang yuanfang qisu zhi fayuan (因动物世界启用人脸识别，浙江一大学教授将园方起诉至法院) [Because the Safari Park Started Using Facial Recognition, A Professor From A University in Zhejiang Took the Park Straight to Court], Baijiahao (Nov. 3, 2019), https://m.thepaper.cn/baijiahao_4856760 (describing how a man sued a safari park for requiring a facial scan, citing a violation of the PRC Consumer Rights Protection Law).

[276] *See* Punjab Safe Cities Authority Act 2016 (Act I of 2016), promulgated by the Punjab Government on Feb. 6, 2016.

[277] Interview with Akbar Nasir Khan, Chief Operating Officer of the PSCA-Lahore, Huawei, https://e.huawei.com/cn/videos/cn/2018/201809111505# (last visited June 8, 2020).

[278] Sebastian Moss, *Huawei signs MoU with Pakistan for cloud data center*, DATA CENTRE DYNAMICS (Apr. 29, 2019), https://www.datacenterdynamics.com/news/huawei-signs-mou-pakistan-cloud-data-center/.

[279] *Id.*

[280] Huawei News Room, *Huawei Announces Safe City Compact Solution to Protect Citizens in Small and Medium Cities*, HUAWEI (Oct. 15, 2018), https://e.huawei.com/us/news/smart-cities/201810150942.

[281] *See* Moss *supra* note 278.

[282] See interview with public interest lawyer, Lahore, Nov. 27, 2019 (noting that the power to remove Internet content lies with the Pakistan Telecommunications Agency under section 37 of the Prevention of Electronic Crimes Act of 2016).

the police, military, and intelligence agencies seek to expand their intelligence-gathering capacities through Chinese technology, they may be subordinating themselves to an even greater data-gathering and data-control system, orchestrated by China's intelligence-gathering capabilities.

Nonetheless, under CPEC, additional "safe city" projects are underway in Islamabad, Peshawar, Karachi, Gwadar, and Quetta.[283] These safe cities will be interlinked as part of what the *Long Term Plan* calls "information network infrastructure" for managing data in the country.[284] Such interlinkage further exemplifies principle 8 of the Digital Initiative, specifically, the promotion of "digital economic cooperation between cities" (*tuidong chengshi jian de shuzi jingji hezuo*).[285] A corridor from Gwadar in southern Pakistan to Kashgar in western China connected through "safe" and "smart" cities is one way that CPEC aspires to integrate the two economies.[286]

C. Pakistan's Emerging Data Governance Regime

Chinese technology companies in Pakistan or elsewhere must comply with local law. However, because of the relative nascence of Pakistani data law, to date, it provides little safeguard against foreign intrusion and control. The existing rules function more to enhance police powers and the reach of intelligence services than to protect citizens' data privacy. There is a latent convergence between Pakistani and Chinese approaches to data governance that CPEC catalyzes. Pakistan has high demand for sophisticated digital infrastructure under a political system that prioritizes social stability. One consequence of this combination is that the development of Pakistan's digital infrastructure may be accelerating more quickly than its data-related legal infrastructure. These ingredients make Pakistan ripe for the Beijing Effect.

In recent years, there have been significant debates in Pakistan about cybersecurity and privacy. On the one hand, the country has been entrenched for decades in a fight against terrorism, and thus, there is a strong prerogative placed on national security, including governmental access to data.[287] On the other hand, Pakistan features an active judiciary that has produced an extensive jurisprudence of "fundamental rights," which include privacy.[288] This dynamic is also palpable within the Constitution of Pakistan itself as it protects privacy but also subsumes such "fundamental rights" under

---

[283] Talal Raza, *Exclusive: The CPEC Plan for Pakistan's Digital Future*, DIGITAL RIGHTS MONITOR (Oct. 13, 2017), https://digitalrightsmonitor.pk/exclusive-the-cpec-plan-for-pakistans-digital-future/.
[284] *See supra* text accompanying note 248.
[285] *See supra* text accompanying note 233.
[286] *See* Husain *supra* note 248.
[287] AYESHA SIDDIQA, MILITARY INC.: INSIDE PAKISTAN'S MILITARY ECONOMY (2017) (analyzing how the military controls the country).
[288] *See* MUHAMMAD AZEEM, LAW, STATE, AND INEQUALITY IN PAKISTAN: EXPLAINING THE RISE OF THE JUDICIARY 92, 127, 203 (2017) (chronicling the contested jurisprudence on "fundamental rights," stemming from their recognition in the 1956, 1962, and 1973 Constitutions).

the Armed Forces' and police' prerogative to maintain "public order."[289] These debates shape the regulatory landscape on data governance in Pakistan.

In parallel with China's disaggregated regulatory regime,[290] there are a number of Internet regulators in the country: the Pakistan Telecommunications Authority (PTA), the Federal Investigation Agency, the Supreme Court of Pakistan, and the Ministry of Information Technology, as well as the Web Evaluation Cell (WEC), established by the Ministry of Religious Affairs and Inter-Faith Harmony. These bodies are responsible for governing Pakistan's cyberspace with an emphasis on blocking potentially subversive material deemed anathema to national security and to Islam. The most important of these is the PTA, which regulates all telecommunications systems and services in the country and serves as a gatekeeper. For example, upon the WEC's recommendation, the PTA blocked 6,149 websites in 2017.[291] In 2019, the PTA blocked 900,000 URLs for "reasons such as carrying blasphemous and pornographic content and/or sentiments against the state, judiciary or armed forces."[292] Beyond Internet filtering, the PTA has also sought to regulate the use of encryption software and Virtual Private Networks (VPNs).[293] The PTA's monitoring extends to all mobile phones brought into the country through a new tax system that requires anyone entering the country to register their phone, if they are not using a foreign SIM card.[294]Additionally, the National Database and Registration Authority (NADRA) controls a centralized repository of citizen data.[295] It has suffered data leaks that caused widespread identity theft due to its reliance on vulnerable e-government mobile apps.[296] NADRA's database is interlinked with "safe city" projects like those led by the PSCA, which allows authorities to surveil citizens.[297] In summary, Pakistan's demand for cutting-edge digital infrastructure under governmental control

[289] *See* The Constitution of Pakistan, effective Aug. 14, 1973, Part II, Ch. 1, art. 14(1) (providing that the "dignity of man, and, subject to law, the privacy of home, shall be inviolable). *But see* art. 8 (providing "laws relating to members of the Armed Forces, or of the police or of such other forces as are charged with the maintenance of public order" are not void if they are inconsistent with fundamental rights).
[290] *See supra* text accompanying note 87.
[291] Staff Report, *6,149 Websites Blocked in Pakistan by PTA*, PAKISTAN TODAY (June 2, 2018), https://www.pakistantoday.com.pk/2018/06/02/6149-websites-blocked-in-pakistan-by-pta/.
[292] Kalbe Ali, *900,000 Websites Blocked over Content, Says PTA*, DAWN (Sep. 27, 2019), https://www.dawn.com/news/1507590.
[293] Hija Kamran, *PTA Restricts Access to 11,000 Proxy Servers; Aims to Regulate VPN use in Pakistan 'Through a New Model'*, DIGITAL RIGHTS MONITOR (July 19, 2019), https://digitalrightsmonitor.pk/pta-restricts-access-to-11000-proxy-servers-aims-to-regulate-vpn-use-in-pakistan-through-a-new-model/.
[294] Ashfaq Ahmed, *Traveling to Pakistan? Then You Must Register Your Mobile Phone*" GULF NEWS (Jan. 23, 2019), https://gulfnews.com/world/asia/pakistan/travelling-to-pakistan-then-you-must-register-your-mobile-phone-1.61621236.
[295] *See* National Database and Registration Authority Ordinance 2000 (Ordinance VIII of 2000), Gazette of Pakistan, Extraordinary, Part I, Mar. 10, 2000 (empowering NADRA to establish a nation-wide registration system for all citizens).
[296] Jannat Ali Kalyar, *Cyber insecurity*, THE NEWS ON SUNDAY (Dec. 22, 2019), https://www.thenews.com.pk/tns/detail/586618-cyber-insecurity.
[297] *Id.* (describing how a couple who were engaged in intimate acts in a car were identified by the government).

occurs against the backdrop of a legal infrastructure that, where it exists, supplements the state's "stability imperative," to use an expression from Chinese legal studies.[298]

Pakistan suffers from a paucity of rules governing interactions between data subjects, data controllers and data processors, including but not limited to telecommunication and ISPs, e-businesses, financial institutions, and government services portals.[299] Existing legislation grants wide-ranging powers to authorized officers to conduct search and seizure of data[300] and mandates that ISPs must retain data of users for a minimum period of one year.[301] The Pakistan Telecommunication (Re-organization) Act, 1996,[302] which was promulgated following the introduction of cellular services and the Internet in Pakistan, authorizes the government to monitor digital communications and limits the use of encryption technology.[303]

The 2016 Prevention of Electronic Crimes Act (PECA) is the main legislation on cybercrime. The PECA includes a broad and long list of offenses, including *inter alia* cyberterrorism, hate speech, unauthorized use of identity information, unauthorized use of SIM cards, child pornography, malicious cod, cyberstalking, spamming, and spoofing. The PECA imposes strict penalties. Those found guilty of spoofing, for instance, face imprisonment of up to three years, a five hundred thousand rupee fine (about $6,600), or both.[304] Many of the enumerated offenses go well beyond international norms, such as those in the Council of Europe Convention on Cybercrime ("Budapest Convention"), to which neither Pakistan nor China are parties.[305] In terms of enforcement, the PECA solidifies the PTA's position as the main inter-ministerial body for regulating digital media. Section 32 of the PECA grants wide powers to the PTA to block "unlawful online content" if the PTA considers doing so would be in the interest of the "glory of Islam or the integrity, security or defence of Pakistan."[306] In these instances, the PTA is also authorized to conduct search and seizures of data, without judicial oversight.[307]

Lastly, as a result of the monitoring of Pakistan's combatting of money laundering and terrorist financing by the Financial Action Task Force (FATF), Pakistan has promulgated the Securities and Exchange Commission of Pakistan Search and

---

[298] SARAH BIDDULPH, THE STABILITY IMPERATIVE: HUMAN RIGHTS AND LAW IN CHINA (2015) (arguing that in China, law serves to protect "social stability" (*weiwen*)).
[299] BYTES FOR ALL, ELECTRONIC DATA PROTECTION IN PAKISTAN: WHAT NEEDS TO BE DONE? (2017), https://bytesforall.pk/sites/default/files/Data_Protection_in_Pakistan.pdf.
[300] Prevention of Electronic Crimes Act, 2016, sec. 32.
[301] *Id.*
[302] Pakistan Telecommunications (Re-organization) Act, 1996 (Act No. XVII of 1996).
[303] Umer Gilani and others, 'Electronic Data Protection in Pakistan: What Needs to be Done?' (Bytes for All, Pakistan 2017).
[304] Prevention of Electronic Crimes Act, 2016, promulgated by the Majlis-E-Shoora (Parliament) on Aug. 11, 2016, §23.
[305] *See* Convention on Cybercrime, Budapest, ETS No. 185 (Nov. 23, 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
[306] Prevention of Electronic Crimes Act, 2016, *supra* note 304, at §34.
[307] *Id.*, at §32 (providing far-ranging powers to authorized officers to conduct search and seizure of data).

Seizure Rules 2019 ("SECP Rules").[308] The SECP Rules establish a procedure for the use of powers by the SECP to carry out search and seizure of any property in order to identify deceptive practices in the corporate sector. The SECP Rules allow an investigating officer to access, seize and secure electronic devices and allows them to have access to any passwords necessary to operate electronic devices.[309] Thus, even legislation meant to implement international standards such as those promulgated by the FATF may eventually increase the discretionary powers of regulatory authorities at the expense of individual's data privacy.

The coupling of a growing demand for digital infrastructure that enhances state access to data with a thin legal infrastructure is highlighted by the fact that Pakistan lacks a data protection law. A draft "Personal Data Protection Bill" languished in Parliament and had severe flaws. In the words of a member of a Pakistani civil society group:

> The first draft of the Data Protection Bill, dated July 2018, had an explicit exception for government bodies and personal data held by government bodies. In other countries, the biggest problem is private companies holding data, but in Pakistan, citizen data is held by the state (e.g., biometric data) and [in] the NADRA database. So the government is unwilling to make itself accountable. This exception was removed in a later draft, but [one] can [still] see huge exceptions granted.[310]

The 2020 draft of the Personal Data Protection Bill makes a data subject's consent to the processing of her data mandatory,[311] but provides a list of broad exceptions to this rule, including "for the exercise of any functions conferred on any person by or under any law."[312]

The picture that emerges from the combination of a heavy demand for digital infrastructure without a robust legal framework, is not one of China imposing its model on Pakistan; instead, Pakistan and China demonstrate congruence in approaches to data governance, facilitated by Pakistan's reliance on Chinese-built and -operated infrastructure. This convergence is far from inevitable, however. The "digital authoritarianism" thesis tends to assume that authoritarians are interchangeable and that China's data governance approach can be "exported." Neither assumption holds in the case of Pakistan, which features a strong military but also has a multi-party democratic system, an interventionist judiciary, a raucous press, a liberal civil society, activist labor

---

[308] Securities and Exchange Commission of Pakistan (Search and Seizure) Rules, 2019, issued by the Government of Pakistan Securities and Exchange Commission (Jul. 1, 2019), https://khilji.net.pk/wp-content/uploads/2019/07/Search-and-Seizure-Rules-2019.pdf.
[309] *Id.*, at §7.
[310] Interview, Lahore, Nov. 27, 2019.
[311] Personal Data Protection Bill 2020, Ministry of Information Technology & Telecommunication, Draft April 9, 2020, art. 5.1, https://moitt.gov.pk/SiteImage/Misc/files/Personal%20Data%20Protection%20Bill%202020%20Updated(2).pdf.
[312] *Id.*, at 5(2)(g).

unions, and a cosmopolitan Muslim population that may at least complicate the adoption of Chinese data governance approaches.

For example, in March 2012, the Pakistan government published a request for proposal for a project consisting of the "development and operation of a national level URL Filtering and Blocking System."[313] Case law at the time shows that the judiciary regarded Chinese legislation as a model for blocking blasphemous content on the Internet.[314] Activists, however, scuttled the plan for the nation-wide filtering system. Using a shaming strategy, these Pakistani activists were able to ensure that five of the world's leading technology companies would not supply the digital infrastructure for the filtering system.[315] Of the three tech companies that remained silent, two were Chinese and one was Canadian. Ultimately, a modified filtering system was established via the Canadian company;[316] the civil society resistance had colored popular perception about the "China model" as one unattractive for Pakistan.

While a wholesale exportation of China's data governance to countries like Pakistan is not feasible, an incremental and increasing reliance on Chinese digital infrastructure is plausible. Pakistan is eager to construct and rely on China-made digital infrastructures such as fiber-optic cables, data centers, e-commerce platforms, and satellite systems.[317] Critically, it is Chinese companies that are providing these infrastructures. For instance, in 2017, the PTA inaugurated the Pakistan Internet Exchange Point (known as PKIX), ensuring that all data, either generated within Pakistan or flowing through the country, must be funneled through a single interface between ISPs and content providers, located in Islamabad. Internet exchange points are core Internet infrastructure, which has been historically lacking in the Global South, and are also vectors for surveillance.[318] PKIX, like the submarine cable system PEACE, is powered by Huawei.[319] China's ICT giant operates the heart of Pakistan's Internet infrastructure.

Countries like Pakistan seek to emulate China's approach to data governance centered around "data sovereignty." However, because the Chinese companies that are

---

[313] Pakistan's National ICT R&D Fund, *Request for Proposals: National URL Filtering and Blocking System* (Feb. 22, 2012), https://info.publicintelligence.net/PakistanFiltering.pdf.
[314] *See* 2012 CLC 1300 [Lahore] Islamic Lawyers Movement vs. Federation of Pakistan (suggesting that "the government should strive for legislation in such regard as the lines already adopted by other Islamic countries in addition to China").
[315] Michael Newman, *Say No to Government Censorship of the Internet in Pakistan*, BUSINESS & HUMAN RIGHTS RESOURCE CENTRE (Mar. 2, 2012), https://www.business-humanrights.org/en/statement-by-websense-say-no-to-government-censorship-of-the-internet-in-pakistan-regarding-call-by-pakistan-govt-for-proposals-for-a-filtering-and-blocking-system.
[316] Jakub Dalek et al., *O Pakistan, We Stand on Guard For Thee: An Analysis of Canada-Based Netsweeper's Role in Pakistan's Censorship Regime*, THE CITIZEN LAB (Jun. 20, 2013), https://citizenlab.ca/2013/06/o-pakistan/#8.
[317] *See supra* §IV.A–B.
[318] *See* Fernanda R. Rosa, GLOBAL INTERNET INTERCONNECTION INFRASTRUCTURE: MATERIALITY, CONCEALMENT, AND SURVEILLANCE IN CONTEMPORARY COMMUNICATION (2019) (discussing governance *by* internet exchange points and the social, political, and public values at stake).
[319] A second PKIX location, operated by the Internet Society (ISOC), opened in Karachi in Feb. 2019. *See* http://www.pkix.pk/locations.html (last visited Aug. 17, 2020).

building and operating the digital infrastructure are inextricably intertwined with the party-state, and may share data with Beijing when requested to do so, such data sovereignty is ultimately illusory. Experts in Pakistan suspect, at a number of levels, that Pakistan is ceding its sovereignty to China: from Chinese-built infrastructure not only permitting leakage but also allowing for the seeding of disinformation to Islamabad yoking itself to Beijing's policies on cyber issues, whether at the UN, ITU, or Shanghai Cooperation Organization.[320] While there is circumstantial evidence of intrusion, Chinese control of data is not a foregone conclusion. For example, the relationship between the PTA and Tiktok evinces increasing regulatory discoordination if not competition as "governors of speech."[321] Tiktok's censor appears, to the Pakistani authorities, to be potentially both over-inclusive and under-inclusive.[322] As to the latter, lawsuits have been filed to ban Tiktok from Pakistan.[323] In October 2020, the PTA banned Tiktok and then eleven days later, unbanned it.[324] Lawyers familiar with the incident report that rather than evincing Chinese intervention, the episode demonstrates internal political struggles particularly as the PTA, in line with the wishes of the military establishment, seeks to control the public sphere.[325] In summary, the fraught relationship between TikTok and the PTA shows the high degree of regulatory uncertainty Chinese investors face in countries like Pakistan. It also illustrates limits to China's ability to control data governance beyond its borders.

V. Evaluating the Beijing Effect: Data Sovereignty and Digital Development

In the COVID-plagued summer of 2020, concerns over data collection by Chinese companies led to forceful governmental responses outside the BRI. India banned certain Chinese apps outright, citing sovereignty and security concerns.[326] The U.S. government followed suit by announcing prospective restrictions on TikTok and WeChat.[327] These

---

[320] Telephonic interview with Islamabad-based lawyer, March 9, 2019.
[321] *See* Klonick *supra* note 166.
[322] *Compare* Zaheer Ali Khan, *TikTok blocks 93,000 Accounts with "Objectionable Content" in Pakistan*, SAMAA (Sept. 16, 2000), https://www.samaa.tv/news/pakistan/2020/09/tiktok-pakistan-block/ (finding that while the PTA requested that TikTok block 93,000 accounts, TikTok blocked 5.6 million videos and links on its own initiative, indicating the considerable enforcement powers exercised by the company) *with* Anon., *Lahore High Court moved for ban on TikTok app*, DAWN (Aug. 4, 2019), https://www.dawn.com/news/1497950 (describing a lawsuit in the Lahore High Court to ban TikTok on the grounds that it publicizes pornographic and illegal material).
[323] *See e.g.*, *id* and Sajjad Haider, *Petition to Ban Tiktok filed in the Peshawar High Court*, SAMAA (Sept. 8, 2020), https://www.samaa.tv/news/2020/09/tiktok-ban-in-pakistan-petition/ (indicating how a suit was brought against Tiktok on the basis of its "immoral and objectionable" content).
[324] Meher Ahmad, *Who's Afraid of a Meme? Pakistan's TikTok Ban is Not Like the Ones in Other Countries*, RESTOFWORLD (Oct. 16, 2020), https://restofworld.org/2020/who-is-afraid-of-a-meme/. *But see* Manish Singh, *Pakistan Lifts Ban on TikTok*, TECHCRUNCH (Oct. 19, 2020), https://techcrunch.com/2020/10/19/pakistan-lifts-ban-on-tiktok/.
[325] Telephonic interviews with Pakistani lawyers, 28 Oct. and unli2 Nov. 2020.
[326] Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat*, NY TIMES (June 29, 2020), https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html.
[327] Exec. Order on Addressing the Threat Posed by TikTok (Aug. 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/; Exec.

moves can be seen as responses to the Beijing Effect: if China's growing influence on transnational data governance is the concern, limiting the operation of Chinese companies in major markets may appear to be an effective counter strategy. While India's decision is in line with a broader agenda that seeks to retain Indian data as a strategic resource,[328] the U.S. contradicted long standing but increasingly contested commitments towards free data flows and "Internet freedom."[329] However, pushing Chinese companies out of major markets might only strengthen their reliance on third countries, which continue to welcome their activity, thereby inadvertently reinforcing the Beijing Effect. Moreover, the stated concerns about Chinese data-gathering in the U.S. ring hollow considering U.S. companies' data collection practices in the absence of comprehensive federal data privacy and cybersecurity legislation. In what follows, we focus on two key aspects that explain developing countries' growing demand for Chinese digital infrastructure and the Chinese approach to data governance–the dual promise of data sovereignty and digital development–and expose its inherent contradictions. On this basis, we caution against building digital infrastructures without appropriate legal infrastructures.

A. The Appeal and Limits of Data Sovereignty

Different versions of "data sovereignty" have been invoked by Native American tribes in the U.S.,[330] promoters of innovative urban data governance projects in the EU,[331] exponents of India's evolving digital industrial policy,[332] and others. Such variegated mobilization of the term may be unsurprising given that "data sovereignty" combines elements of under-specified concepts. There is no universally accepted definition of the term. As a result, its usage, appeal, and limitations need to be carefully examined in the context in which it is being deployed.

China has emerged a champion of a particular version of "data sovereignty" in continuation of its invocation of "cyber sovereignty" in Internet governance institutions. This is not to suggest a linear development as the Chinese coinage of the term has been in flux and is entangled with China's complicated historical relationship to "sovereignty."[333] "Cyber sovereignty" was meant to challenge U.S. hegemony in Internet governance and pushed back against notions of "cyber anarchy" and "cyber libertarianism" that suggested that the Internet was fundamentally unregulatable by governments. "Data sovereignty" is

---

Order on Addressing the Threat Posed by WeChat (Aug. 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

[328] Draft National e-Commerce Policy, India's Data for India's Development (Feb. 23, 2019), https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

[329] *See* Jack Goldsmith, *The Failure of Internet Freedom*, KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY (June 13, 2018), https://knightcolumbia.org/content/failure-internet-freedom.

[330] *See, e.g.* Rebecca Tsosie, *Tribal Data Governance and Informational Privacy: Constructing "Indigenous Data Sovereignty,"* ARIZONA LEGAL STUDIES DISCUSSION PAPER NO. 19-19 (Sep. 2019).

[331] *See* https://decodeproject.eu/ (last visited Aug. 17, 2020).

[332] *See* Report by the Committee of Experts on Non-Personal Data Governance Framework (July 12, 2020), https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf.

[333] *See* Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization, in:* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107 (Dennis Broeders and Bibi van den Berg, eds., 2020); MARIA ADELE CARRAI, SOVEREIGNTY IN CHINA, A GENEALOGY OF A CONCEPT SINCE 1840 (2019).

congruent with these notions in confronting the global dominance of U.S. actors in terms of data collection capacity and in asserting governmental authority over cross-border and in-country data flows. The shift in emphasis from "cyber" to "data" is significant as it signals the recognition of data's paramount importance in the early twenty-first century. Data is both a resource for economic development, in particular, as an input factor for machine learning algorithms, and a tool for governance in a digitalized society. China's invocation of "data sovereignty" echoes these sentiments and imbues them with the party-state's objective of social control.[334]

Data sovereignty's core tenets of governmental control, self-determined economic development, and social order have considerable appeal for countries around the world and are not necessarily limited to nondemocratic governments. To the extent to which these ambitions limit cross-border data flows, they come into tension with the Internet's potential to facilitate global interconnectedness. If "data sovereignty" is invoked to control and censor intra- and inter-country data flows, the Internet's erstwhile promise as a liberating force is being undermined. These tradeoffs and drawbacks of "data sovereignty" are well recognized.[335] They are, however, unlikely to sway countries that emulate China's data sovereigntist policy prescriptions since governmental control over data flows for economic, social, or political purposes is the point, at the expense of imposing negative externalities on global interconnectedness and certain individual rights.[336]

It is also well understood that conceptions of "cyber sovereignty," and, by extension, "data sovereignty," that seek to (re)territorialize data qua data localization, as China does, do not map neatly onto the Internet's architecture of inter-connected "autonomous systems."[337] Even China's sophisticated cross-border data flow control infrastructure does not lead to a perfect re-alignment between physical borders (between territories) and virtual borders (between networks). Yet, neither "cyber sovereignty" nor "data sovereignty" require such congruence to achieve their objectives.

Indeed, sovereignty has never been absolute and can only be achieved and exercised to varying degrees, thereby exposing the sovereign equality of states as a mere principle, not a description of reality, if not "organized hypocrisy."[338] Data sovereignty is no exception and it is this dimension of unequal power to which we want to draw attention. If our contention that the Beijing Effect is driven by host states' aspirations towards "data sovereignty" is correct, they need to reckon with the inherent limitations of "data sovereignty" in a still interconnected world. As Henry Farrell and Abe Newman

---

[334] *See supra* text accompanying note 86.
[335] *See* Andrew Keen Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 360–366 (2018) (providing a descriptive account of data sovereignty encompassing supreme control over a territory independently from other sovereigns).
[336] Eyal Benvenisti, *Sovereigns as Trustees of Humanity*, 107 AM. J. OF INT'L LAW 295 (2013) (arguing for a conception of sovereignty that requires recognition and, if possible, avoidance of imposing externalities transnationally).
[337] *See* Milton Mueller, *Against Sovereignty in Cyberspace*, INTERNATIONAL STUDIES REVIEW (2019), viz044 (arguing that applying sovereignty to cyberspace is "inappropriate to the domain").
[338] STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY (1999).

have shown, interconnected networks create structures of interdependence that can be weaponized by those who control the relevant infrastructure.[339] They identify the "panopticon effect," which allows for extensive information gathering, and the "chokepoint effect," through which network access can be denied. As China increasingly supplies digital infrastructures through the DSR, its ability to leverage this kind of infrastructural power grows. This is particularly worrisome from the U.S. perspective,[340] as the U.S. has enjoyed hegemony over global networks since WWII and explains why the U.S. is so adamant in organizing opposition against Huawei's involvement in 5G expansion.

From the perspective of developing countries, such as Pakistan, however, the situation is less straightforward. "Weaponized interdependence" is a function of uneven control over digital infrastructures. The creation of alternative infrastructures exceeds most states' capacity; even the EU's prospects in creating an alternative cloud infrastructure seem uncertain at best.[341] At the same time, digital isolationism is hardly an appealing option given the perceived economic, social, and political appeal of the digital transformation. It follows that the degree of "data sovereignty" available to developing countries is determined by factors such as their technological capacity, economic power, and the sophistication and effectiveness of their legal system.

Governmental control over data flows depends not just on territorial control over data (which can be achieved through territorial data localization) but also requires effective control over the corporations that build, operate, and maintain the relevant infrastructure. This holds generally true irrespective of a given company's country of origin (indeed, it also applies to domestic firms). To the extent to which Chinese companies operate under the control of the CCP when providing digital infrastructure abroad, they undermine the "data sovereignty" to which host states of the DSR aspire. Chinese SOEs are extensions of the Chinese state, even if some operate as their own empires and thus may be more autonomous from Beijing than others. The question of whether or to what extent the nominally private companies follow party diktats is a live issue about which we cannot provide definitive evidence. Anecdotal evidence suggests that some firms may refuse access to data requests in certain contexts.[342] Nonetheless, initial fieldwork with legal service providers to Chinese companies operating in emerging economies suggests that even private companies must exercise what is known as "emulation consciousness" (*kanqi yishi*), or as one interlocutor put it, "align with your

[339] Henry Farrell and Abe Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L SECURITY 42 (2019).
[340] Stephanie Kirchgaessner, *Revealed: China Suspected of Spying on Americans Via Caribbean Phone Networks*, THE GUARDIAN (Dec. 15, 2020), https://www.theguardian.com/us-news/2020/dec/15/revealed-china-suspected-of-spying-on-americans-via-caribbean-phone-networks.
[341] *See* https://www.data-infrastructure.eu/ (last visited Aug. 17, 2020).
[342] Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE (Apr. 2, 2020), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement (providing examples of Chinese companies Didi, Tencent, and Alibaba refusing governmental requests for data).

leader, the Supreme One, President Xi."[343] When push comes to shove, the party-state brooks no disobedience.

Developing countries are likely aware of these factors, yet their demand for Chinese digital infrastructure is growing. The Beijing Effect is, in this regard, a function of the declining appeal of U.S.-provided digital infrastructure. The Snowden revelations shattered trust in the U.S. as global steward for free data flows. U.S. technology companies have (at least so far) enjoyed a relatively high degree of freedom in their global operations; some have even sought to position themselves as neutral "Digital Switzerlands."[344] Yet they cannot escape demands by their home jurisdiction, whether in form of access to transnational data requests under the CLOUD Act or through other tools at the disposal of U.S. national security agencies. Moreover, their global dominance – only rivaled by Chinese companies – and unabashed hunger for data invokes concerns over data extractivism in continuation of colonialist patterns of capitalism.[345] The best strategy to counter the Beijing Effect is arguably to diminish the relative appeal of Chinese digital infrastructure by providing alternatives that cater to the demands of host states while creating credible legal and technological safeguards against the panopticon and chokepoint effects and the excesses of "surveillance capitalism" to re-establish trust. In the absence of such counter strategies, host states interested in data sovereignty and digital development may well prefer Chinese over U.S. digital infrastructure.

B. The Digital Silk Road and Digital Development

The second main driver of the Beijing Effect is the promise of digital development. The World Bank and other development organizations have been key proponents of the transformation of economies through technological innovation, accessible digital infrastructure, and open and universal governance frameworks.[346] Through the BRI, which is fundamentally a development project and the DSR, in particular, the Chinese party-state and Chinese enterprises offer their own version of digital development. This path depends on making digital infrastructure accessible but its governance framework nominally operates to concentrate control of data in the host government. The assertion of governmental control over data flows is in tension with development models that emphasize the "free flow" of data,[347] , but the PRC's success in developing its digital economy lends credence to the DSR's promise to enable economic

[343] E-mail correspondence between lawyer who assists Chinese companies in their overseas deals and [author], Apr. 7, 2020.
[344] Kirsten Eichensehr, *Digital Switzerlands*, 167 U. PENN. L. REV. 665 (2019).
[345] *Contrast* NICK COULDRY AND ULISES ALI MEJIAS, THE COSTS OF CONNECTION: HOW DATA IS COLONIZING HUMAN LIFE AND APPROPRIATING IT FOR CAPITALISM (2019) (emphasizing continuities) *with* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2020) (highlighting differences between surveillance capitalism and prior forms of capitalism).
[346] World Bank, Digital Development, https://www.worldbank.org/en/topic/digitaldevelopment/overview#2 (last viewed Aug. 17, 2020).
[347] *See* James Manyika et al, *Digital Globalization: The New Era of Global Flows* (February 4, 2016), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows; Martina Ferracane and Erik van der Marel, *Do Data Policy Restrictions Inhibit Trade in Services?*, ECIPE DTE WORKING PAPER 2 (October 2018).

growth. Chinese e-commerce platforms, in particular, are being touted as important infrastructures for small and medium-sized enterprises.[348]

We cannot assess the economic impact of the DSR generally or on countries like Pakistan in particular, but we sound a cautionary note from the perspective of law and development. As a general observation, the Beijing Effect may have disparate impact on host state legal development. On the one hand, it is conceivable that enhanced digital infrastructure could catalyze access to legal infrastructures just as digital development fosters access to markets.[349] For example, cost-effective online dispute resolution for e-commerce could better protect consumers' rights than offline analogues. Increasingly automated contracts could change the need for legal services. In the aggregate, private governance systems of digital supply chains could interlink economies and lower barriers to entry.[350] The integration of law and technology by building on digital infrastructures could represent one of the "alternative development strategies" for which David Trubek, one of the founders of the study of law and development, has long been searching.[351]

Despite the foregoing, we question the feasibility of replicating China's data-driven development strategy and caution against a digital transformation without appropriate safeguards. The Beijing Effect seems, to a significant extent, animated by a desire to emulate China's transition towards a highly digitalized economy. In this context, it is important to bear in mind the unique features of the PRC, most notably its massive consumer base, which makes it feasible to develop a digital ecosystem that aspires towards a relatively high degree of independence from foreign companies and subjects those that are allowed to operate within China to a regulatory straightjacket. Some have attributed the relatively rapid rise of China's digital economy to a lack of law, in particular in terms of intellectual property law enforcement, which reputedly enabled cut-throat competition, innovation, and growth.[352] While this might lend credence to those who have criticized the advisability of strong intellectual property protections for economic development, it would be misguided to attribute China's economic success to this element in isolation. Economic development is always entangled with legal structures of various kinds.[353] Within the PRC, Chinese companies have sometimes resorted to

---

[348] *See* THE WORLD BANK AND ALIBABA GROUP, E-COMMERCE DEVELOPMENT: EXPERIENCE FROM CHINA (2019), https://documents.worldbank.org/en/publication/documents-reports/documentdetail/823771574361853775/overview (touting the beneficial effects of Taobao Villages).
[349] *See* GILLIAN HADFIELD, RULES FOR A FLAT WORLD (2016) (suggesting that outdated legal infrastructures ought to be replaced by leveraging digital technologies).
[350] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, DIGITAL ECONOMY REPORT 2019 130 (2019) (citing the example of how the digital economy has empowered Haitian women's micro-enterprises).
[351] David M. Trubek, *The 'Rule of Law' in Development Assistance: Past, Present, and Future*, *in* THE NEW LAW AND ECONOMIC DEVELOPMENT 74, 93 (David M. Trubek & Alvaro Santos eds., 2006).
[352] Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563 (2018) (arguing that private actors like Taobao make their own law in China); KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY AND THE NEW WORLD ORDER (2018) (suggesting that China's rise in AI is driven by constant pressure to innovate as plagiarism is rampant).
[353] Jedediah Britton-Purdy, David Singh Grewal, Amy Kapczynski & K. Sabeel Rahman, *Building a Law-and-Political-Economy Framework: Beyond the Twentieth-Century Synthesis*, 129 YALE L. J. 1784 (2019).

making "law, Chinese style" by enforcing contracts, resolving disputes, and preventing fraud themselves in the absence of a robust public legal system. But they cannot simply replicate these features of self-governance abroad. To take the Pakistan example, while Pakistani law on data governance may be nascent, the Pakistani market is not a desert of norms. There are state and non-state actors that actively shape the rules, whether legally binding or informal. The political-economic ecosystem of host countries differs—sometimes considerably so—from what Chinese actors are used to and this has implications for the replicability of the Chinese growth story.

Much ink has been spilled about the vices of past efforts at economic development in general, and the dependencies creates by established development institutions and enshrined in legal instruments such as bilateral investment treaties or loan conditionalities. Yet, the Beijing Effect raises concerns about a different kind of dependency incurred by the relatively rapid creation of digital infrastructures in the absence of appropriate legal frameworks. While much attention must be paid to the significant social and political costs that digital infrastructures might impose, for example, when they enable extended governmental control frameworks, there is also an economic development angle to be considered. If developing countries transition towards a digital economy that relies on Chinese digital infrastructure without commensurate legal frameworks (for example, with regard to taxation) to reap the societal benefits, digital development may exacerbate rather than alleviate in-country inequality as the digital transformation creates winners and losers. The fact that Western societies struggle with this very problem does not inspire confidence but makes it even more pressing.

VI. Conclusion

The coronavirus pandemic potentially marks a turning point in the global governance of data.[354] The world is adapting by becoming more dependent on digital technologies to continue business operations in virtual settings. Consequently, data flows are becoming the lifeline of the global economy and demand for and reliance on digital infrastructures is increasing. For these reasons, what we have sought to encapsulate as the Beijing Effect is likely to grow, at least in the near term. As we have argued in this Article, China has a considerable impact on data governance transnationally. This influence is neither a function of China "exporting" a certain "model" nor a dynamic comparable to the "Brussels Effect" under which companies gravitate towards European law. Rather, it is governmental demand for digital infrastructure, and its corollaries, namely, data sovereignty, but also economic development and social order, more generally, that drive China's ascendancy in global data governance.

Yet it seems premature to predict that China's approach to data governance, its emulation by other countries, and the Western response to such developments will

[354] *See also* Kathleen R. McNamara & Abraham L. Newman, *The Big Reveal: COVID-19 and Globalization's Great Transformations*, 74 INTERNATIONAL ORGANIZATIONS 1, 13-15 (2020) (asserting that the pandemic has underscored the importance of digital technologies).

"break" the Internet into different "data realms."[355] Geopolitical struggles over global communication infrastructures are nothing new and the economic case for retaining connectivity is overwhelming. Their differences notwithstanding, the approaches of China, the EU, and U.S. also share important commonalities and hence are not mutually exclusive. Developing countries face difficult choices. While they cannot escape the Beijing Effect nor achieve data sovereignty without foregoing the potential of digital development, they might be able to hedge, that is, to triangulate their relationship to the digital superpowers. As we have argued, a digital development strategy requires the commensurate development of legal frameworks to steer the digital transformation into societally beneficial directions.

[355] Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. OF INTL. ECON. LAW 245 (2018) (claiming that the U.S., EU, and China have created three distinct data realms with different approaches to data governance).