Introduction

Sovereignty 2.0

Anupam Chander and Haochen Sun

The Internet was supposed to end sovereignty. "Governments of the Industrial World, you weary giants of flesh and steel, you have no sovereignty where we gather," John Perry Barlow famously declared.[1] Sovereignty would prove impossible over a world of bits, with the Internet simply routing around futile controls.[2] But reports of the death of sovereignty over the Internet proved premature. Consider recent events:

- In late 2020, on the eve of what was to be the world's biggest initial public offering (IPO) ever, the Chinese government scuttled the listing of fintech provider Ant Group. Before the failed offering, Ant's CEO, Jack Ma, had made what some saw as a veiled critique of the government: "We shouldn't use the way to manage a train station to regulate an airport. . . . We cannot regulate the future with yesterday's means."[3] Chastened after Beijing's intervention, Ant announced that it would "embrace regulation," and Chinese netizens declared Jack Ma duly "tamed."[4]
- In June 2021, France fined Google $593 million for failing to follow an order to negotiate with news publishers to compensate them for displaying snippets of the publishers' news items before linking to them.[5]

[1] *See* John P. Barlow, *The Declaration of the Independence of Cyberspace*, Elec. Frontier Found. (July 16, 2021), https://www.eff.org/cyberspace-independence.

[2] As John Gilmore famously announced, "The Net interprets censorship as damage and routes around it." *See* Philip Elmer-DeWitt, *First Nation in Cyberspace*, Time, Dec. 6, 1993, at 62.

[3] Lily Kuo, *"Jack Ma Is Tamed": How Beijing Showed Tech Entrepreneur Who Is Boss*, Guardian (Nov. 4, 2020), https://www.theguardian.com/business/2020/nov/04/jack-ma-ant-group-is-tamed-social-media-reacts-after-china-blocks-ipo.

[4] *Id.*

[5] *See* Gaspard Sebag, *Google Told to Pay for News with Ultimatum and $593 Million Fine*, Bloomberg (July 13, 2021), https://www.bloomberg.com/news/articles/2021-07-13/google-said-to-be-fined-593-million-by-french-antitrust-agency?sref=CrGXSfHu.

Anupam Chander and Haochen Sun, *Introduction* In: *Data Sovereignty*. Edited by: Anupam Chander and Haochen Sun, Oxford University Press. © Oxford University Press 2023. DOI: 10.1093/oso/9780197582794.003.0001

- In July 2021, Luxembourg's privacy regulator fined Amazon $887 million for data protection violations.[6]
- European Union (EU) authorities are simultaneously investigating Google's ad technology, Apple's App Store, Facebook's Marketplace, and Amazon's use of data from its third-party sellers.[7] Even Facebook Dating receives unwanted attention from the British competition authority.[8]
- The technology giants are not safe even at home, as Ant discovered. In the home of most of the world's largest Internet companies, the U.S. Federal Trade Commission (FTC) seeks to compel Facebook to divest WhatsApp and Instagram, while investigating Amazon for competing with merchants that use its platform.[9] The federal government and all but two U.S. states are bringing antitrust claims against Google,[10] and the U.S. Justice Department is investigating Apple's App Store.[11]
- Assertions of digital sovereignty are hardly limited to Western nations. After Twitter deleted the Nigerian president's tweets warning of a new civil war, the Nigerian government in June 2021 simply banned Twitter from the country. On the eve of an election in January 2021, Uganda went even further, ordering a complete shutdown of the Internet, with President Yoweri Museveni explaining that Facebook had deleted pro-government accounts as manipulative.[12] Uganda followed the example of Zimbabwe, which responded to anti-government protests in 2019 by shuttering the Internet.[13]

[6] *See* Taylor Telford, *E.U. Regulator Hits Amazon with Record $887 Million Fine for Data Protection Violations*, WASH. POST (July 30, 2021), https://www.washingtonpost.com/business/2021/07/30/amazon-record-fine-europe/.

[7] *See* Sam Schechner & Parmy Olson, *Google Faces EU Antitrust Probe of Alleged Ad-Tech Abuses*, WALL ST. J. (June 22, 2021), https://www.wsj.com/articles/google-faces-eu-antitrust-probe-of-alleged-ad-tech-abuses-11624355128.

[8] *See* Press Release, U.K. Competition & Mkts. Auth., CMA Investigates Facebook's Use of Ad Data (June 4, 2021), https://www.gov.uk/government/news/cma-investigates-facebook-s-use-of-ad-data.

[9] Press Release, Fed. Trade Comm'n, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

[10] *See* Press Release, Dep't of Justice, Justice Department Sues Monopolist Google for Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws.

[11] *See* Leah Nylen, *Apple's Easy Fide from U.S. Authorities May be Over*, POLITICO (June 24, 2020), https://www.politico.com/news/2020/06/24/justice-department-anti-trust-apple-337120.

[12] *See* Stephen Kafeero, *Uganda Has Cut Off Its Entire Internet Hours to Its Election Polls Opening*, QUARTZ AFRICA (Jan. 13, 2021), https://qz.com/africa/1957137/uganda-cuts-off-internet-ahead-of-election-polls-opening/.

[13] *See Zimbabwe Imposes Internet Shutdown Amid Crackdown on Protests*, AL JAZEERA (Jan. 18, 2019), https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests.

The state (both nation-state as well as nearly every U.S. state) strikes back.[14] When Thomas Hobbes imagined an "Artificial Man" in the form of a state,[15] he was not picturing Facebook. But the reality is that modern leviathans like Facebook and Google, and even Reddit, Spotify, and Twitter, exercise enormous power over daily life. Increasingly, governments across the world have sought to bring these companies under their control. While China pioneered data sovereignty, it is now the demand of governments from Australia to Zimbabwe. The era of countries unsure whether they had the power to regulate the Internet is over.

Consider, for example, Vietnam's 2018 Law on Cybersecurity, which explicitly declares as its goal the protection of "national cyberspace." Its definition of security includes not just national security, but explicitly also "social order and safety, and the lawful rights and interests of organizations and individuals in cyberspace."[16] While there may be no official signs that one is "Now Entering Vietnamese Cyberspace" to greet visitors, the government clearly believes that Vietnamese cyberspace is not some metaphysical place outside its control.

In February 2022, Vietnam's Southeast Asian neighbor Cambodia suspended its plans to route all Internet traffic into or out of the country through an Internet gateway. Human Rights Watch declared that the true purpose of this infrastructure plan was to "tighten the noose on what remains of internet freedom in the country."[17] Even while suspending its plans, the Cambodian government defended itself, arguing that its goals were to "strengthen national security and tax collection as well as to maintain social order and protect national culture."[18] At the same time, the government insisted, without

[14] For a round-up of some recent enforcement actions faced by the biggest technology companies, *see* Joe Panettieri, *Big Tech Antitrust Investigations: Amazon, Apple, Facebook and Google Updates*, Channele2e (Dec. 24, 2021), https://www.channele2e.com/business/compliance/big-tech-antitrust-regulatory-breakup-updates/.

[15] Thomas Hobbes, Leviathan (1651) ("[A]s men, for the atteyning of peace, and conservation of themselves thereby, have made an Artificiall Man, which we call a Common-wealth; so also have they made Artificiall Chains, called Civill Lawes, which they themselves, by mutuall covenants, have fastned at one end, to the lips of that Man, or Assembly, to whom they have given the Soveraigne Power; and at the other end to their own Ears.").

[16] Vietnam Law of Cybersecurity, art. 6.

[17] Human Rights Watch, *Cambodia Should Scrap Rights-Abusing National Internet Gateway*, May 16, 2022, https://www.hrw.org/news/2022/05/16/cambodia-should-scrap-rights-abusing-national-internet-gateway.

[18] Cambodian Ministry of Foreign Affairs, *Clarification by the Spokesperson of the Ministry of Foreign Affairs and International Cooperation on the National Internet Gateway Establishment*, Feb. 15, 2022, https://www.mfaic.gov.kh/posts/2022-02-15-Press-Release-Clarification-by-the-Spokesperson-of-the-Ministry-of-Foreign-Affairs-and-International-Cooperation-o-10-50-07.

evidence, that such national Internet gateways "prevail in almost all countries around the world."

Against this backdrop, scholars are sharply divided about the increasing assertion of what is called variously "data sovereignty" or "digital sovereignty." Some scholars see it as a natural extension of traditional Westphalian sovereignty to the 21st century.[19] They are joined by other scholars, often from the Global South, who support data sovereignty in order to repulse imperial ambitions for data colonialism, a barricade against the exploitative and extractive practices of Western (and Chinese) technology giants.[20] Other scholars, however, worry that data sovereignty will break the Web apart, jeopardizing its numerous global benefits.[21] As Mark Lemley astutely laments, "The news you see, the facts you see, and even the maps you see change depending on where you are."[22]

This introduction proceeds as follows. Part I reviews some prominent definitions of "digital sovereignty" and "data sovereignty." Part II reviews the rise of digital sovereignty, focusing on four influential jurisdictions (the United States, China, the European Union, and Russia) and also the developing world. Part III describes some ways in which digital sovereignty is different than ordinary terrestrial sovereignty. Part IV considers the struggle for control of cyberspace that followed the Russian invasion of Ukraine. Part V concludes with a sketch of the plan for the volume that follows.

I. Defining Digital Sovereignty

At first glance, the term "sovereignty" over parts of the Internet may seem entirely out of place. After all, one of the prerequisites for the recognition of the sovereignty of a state in international law is the exercise of power over a

[19] *See, e.g.*, Andrew Keane Woods, *Litigating Data Sovereignty*, 128 Yale L.J. 328, 366–71 (2018) (arguing that we should "embrace [] sovereign differences" rather than opt for a single set of rules everywhere).

[20] *See* Renata Avila Pinto, *Digital Sovereignty or Digital Colonialism*, 27 SUR - Int'l J. Hum. Rts. 15, 23–24 (2018); Nick Couldry & Ulises A. Mejias, *Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject*, 20 Television & New Media 336, 337 (2019); *cf.* Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 51 (2019) (noting the distributive nature of the construction of a "biopolitical public domain," where raw data is a resource to be processed).

[21] *See* Mark A. Lemley, *The Splinternet*, 70 Duke L.J. 1397, 1427 (2021) ("[W]e should fight hard not to give up the Internet for an information superhighway, particularly one that's controlled by our national governments.").

[22] *Id.* at 1409.

territory.[23] Andrew Woods grounds his definition of "data sovereignty" in three core elements of state sovereignty: "(1) supreme control; (2) over a territory; (3) independent from other sovereigns."[24] The tension between the notion of "digital sovereignty" and the territorial foundation for sovereignty disappears when one recognizes that in order to exercise control over any territory, it is increasingly necessary to exercise control over the online activities available in that territory. This insight connects place and cyberspace. Woods writes that, in order to control data within their borders to the exclusion of other states, "states can command considerable control over the internet if only because they control the physical components of the network within their borders" through "an impressive arsenal of tools."[25] Dan Svantesson rightly observes that sovereignty should not have to be all or nothing, and so perhaps Woods's requirement of exclusivity is unnecessarily strict for a claim of data sovereignty.[26] For Woods, a state's data sovereignty powers include powers to compel compliance ("leav[ing] companies and their users free to design and use the internet as they see fit, as long as they comply when the government comes knocking") and powers to control the means of compliance ("the state tells internet firms how to operate").[27] It seems clear that multiple states are able to order the same firm how to operate, with occasional conflicts in approaches.[28]

Ke Xu divides sovereignty in cyberspace into three layers: the physical layer (sovereignty over physical Internet infrastructure and activities), the code layer (sovereignty over domain names, Internet standards, and regulations), and the data layer.[29] Like Hobbes, Luciano Floridi begins by theorizing individual sovereignty, which he defines in 21st-century terms as "self-ownership, especially over one's own body, choices, and data,"[30] and

[23] Article 1 of the Montevideo Convention on Rights and Duties of States provides as follows: "The state as a person of international law should possess the following qualifications: (a) a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other states."

[24] Woods, *supra* note 19, at 360.

[25] *Id*. at 360–61.

[26] Dan Svantesson, "*A Starting Point for Re-thinking 'Sovereignty' for the Online Environment*," chapter in this volume.

[27] Woods, *supra* note 19, at 364.

[28] One prominent dispute involving a possible conflict—the Microsoft dispute with the U.S. authorities over data held in Ireland—did not create a hard conflict of laws because Ireland did not explicitly claim that transferring the data to the United States would be illegal under Irish law. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

[29] Ke Xu, *Data Security Law: Location, Position and Institution Construction*, 3 Bus. & Econ. L. Rev. 52, 57 (2019).

[30] Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 Phil. & Tech. 369, 371 (2020).

then extends this to "digital sovereignty," which he defines as the "control of data, software (e.g., AI), standards and protocols (e.g., 5G, domain names), processes (e.g., cloud computing), hardware (e.g., mobile phones), services (e.g., social media, e-commerce), and infrastructures (e.g., cables, satellites, smart cities)."[31]

Data sovereignty, as argued by Paul Rosenzweig, may also be framed as a question: Which sovereign controls the data?[32] The core issue is one of jurisdiction, which is, of course, complicated by the borderless nature of the Internet.[33] "In short, the question is: 'Whose law is to be applied?' "[34] Rosenzweig argues that physical location is, as a practical matter, critical: "Where the servers are and where the data is stored will, in the end, likely control whose law applies. As they say, 'geography is destiny.' "[35] Certainly, the physical control over the network made possible through Internet service providers that route data is a key to digital sovereignty, at least where foreign corporations do not comply on other grounds.

We will use the term "digital sovereignty" to mean the application of traditional state sovereignty over the online domain,[36] or simply "sovereignty in the digital age."[37] Digital sovereignty should be defined broadly to cover a state's sovereign power to regulate not only cross-border flow of data through uses of Internet filtering technologies and data localization mandates, but also speech activities (e.g., combating fake news) and access to technologies. We use the term in a descriptive way to describe efforts by governments to assert control over online activities, often instantiated through actions targeted at Internet intermediaries. Notably, academics and news media are more likely to speak in terms of "data sovereignty" than "digital sovereignty," as a search of the database ProQuest shows:[38]

[31] *Id*. at 370–71.

[32] *See* Paul Rosenzweig, *The International Governance Framework for Cybersecurity*, 37 CAN.-U.S. L.J. 405, 421 (2012).

[33] *See id*.

[34] *Id*. at 422.

[35] *Id*.

[36] This accords with the French Senate investigatory committee report, which defines digital sovereignty as the "capacity of the state to act in cyberspace." LE DEVOIR DE SOUVERAINETÉ NUMÉRIQUE: NI RÉSIGNATION, NI NAÏVETÉ, SENAT (2019), http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2019/2019_Infographies/20191004_infog_Souverainete_numerique_021019.pdf.

[37] Paul Timmers, *Challenged by "Digital Sovereignty,"* 23(6) J. INTERNET L. 1, 18 (2019).

[38] This search run on ProQuest on July 16, 2021, updates an analysis by Stephane Couture & Sophie Toupin, *What Does the Notion of "Sovereignty" Mean When Referring to the Digital?*, 21 NEW MEDIA & SOC'Y 2305, 2306 (2019). Note that the "other" category includes newspapers, trade journals, magazines, reports, blogs, books, and working papers.

	Data Sovereignty		Digital Sovereignty	
	Academic	**Other**	**Academic**	**Other**
2019– June 30, 2023	919	2672	224	1465

It is possible to draw a distinction between "data sovereignty" and "digital sovereignty," where "data sovereignty" refers to control over data, including through data protection law, competition law, and national security law. This definition would make data sovereignty a subset of digital sovereignty. But the relationship between "data sovereignty" thus defined and broader issues such as content moderation quickly becomes difficult to disentangle. Stopping information from flowing across borders, for example, implicates speech and commerce, as well as data governance. Indeed, a distinction between dominion over "data" and dominion over the "digital" is hard to sustain. *In framing this book, we have chosen to use both* "data sovereignty" and "digital sovereignty," recognizing that the term is sometimes used distinctly with "data sovereignty" and sometimes interchangeably. Indeed, we ourselves began the project using the term "data sovereignty," and then adopted the broader term in the course of writing in order to ensure that we captured the breadth of the topic.

II. The Rise of Digital Sovereignty

In this part, we review the effort to attain digital sovereignty in a few key jurisdictions. The review reveals at least three different motivations for assertions of digital sovereignty. First, governments demand digital sovereignty to better protect their population—seeking, for example, to remove material deemed illegal under their laws or to protect the rights of citizens in the digital domain. This often takes the form of regulating foreign corporations that intermediate data flows for the local population. Second, governments seek digital sovereignty in an effort to grow their own digital economy, sometimes by displacing foreign corporations, from fintech to social media. Third, governments seek digital sovereignty to better control their populations—to limit what they can say, read, or do.

A. China: Inventing Digital Sovereignty

In the mid-1990s, when the world started coming online, China's Ministry of Public Security inaugurated its "Golden Shield Project," 金盾工程, which has been described as "a far-ranging attempt to harness emerging information technologies for policing."[39] Henry Gao observed that Chinese digital sovereignty evolved through different phases—physical controls and then controls over the software layer and content.[40] In other words, it went up the Internet stack.[41] As James Fallows wrote in a classic Western account of "the Great Firewall of China," "[i]n China, the Internet came with choke points built in."[42] China takes a multifaceted approach to exerting digital sovereignty, which includes controlling its physical infrastructure, regulating content, balancing negative economic impacts, and building international support for its conception of digital sovereignty.[43] The most prominent aspect of China's physical infrastructure innovation is the "Great Firewall," which is used by the government to block access to content for users in China.[44] However, sometimes the firewall causes collateral impact on Internet freedom beyond China's borders through domain name system pollution, where Chinese domain name servers accidentally serve foreign users, thus inadvertently blocking access to websites by users in other countries.[45]

In 2010, the Chinese State Council officially declared its support for "Internet sovereignty" (*wangluo zhuquan* or 网络主权) in a white paper entitled "The Internet in China." The white paper declared, "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected."[46] The link

[39] Lorand Laskai, *Nailing Jello to the Wall*, *in* JANE GOLLEY, LINDA JAIVIN, & LUIGI TOMBA, CONTROL 192, 194 (2017).

[40] Henry Gao, *Data Regulation with Chinese Characteristics*, *in* BIG DATA AND TRADE 245, 248 (ed. Mira Burri, 2021) (noting that 1996 and 1997 Chinese "regulations all focused on the Internet hardware," while attention was paid later to software and content).

[41] The architecture of the Internet is often described as consisting in stacked layers, from the physical infrastructure to the applications and uses that run atop that infrastructure. *See* Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1742 (2013).

[42] James Fallows, *The Connection Has Been Reset*, ATLANTIC (Mar. 2008), https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/.

[43] Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 403 (2020); *Protecting Internet Security*, CHINA.ORG, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm (last visited Jan. 14, 2022).

[44] *See* Wang, *supra* note 43, at 408, 439.

[45] *See id.* at 408, 439–41; Robert McMillan, *China's Great Firewall Spreads Overseas*, COMPUTERWORLD (Mar. 25, 2010), https://www.computerworld.com/article/2516831/china-s-great-firewall-spreads-overseas.html [https://perma.cc/E2U5-FBHP] (archived Jan. 9, 2022).

[46] *See* Wang, *supra* note 43, at 397.

to territoriality seems to be both a nod to international law and also part of a long-standing Chinese Communist Party official approach to international relations that pledged non-interference in the internal affairs of foreign countries.[47] In 2015, President Xi explained that "respecting cyber-sovereignty" meant "respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace — avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries."[48]

China escalated the tech cold war. The Cybersecurity Administration of China opened investigations into the data transfer practices of Chinese tech giant Didi immediately following that company's New York Stock Exchange listing. It then ordered Didi removed from Chinese app stores.[49] Even though Didi's stock price plummeted, Chinese media celebrated the "rise of data sovereignty."[50]

China's conception of digital sovereignty is rooted, Anqi Wang writes, in traditional notions of territorial sovereignty[51] and officially justified by concern for national and ideological security.[52] China supports a "state-centric multilateralism" model of Internet governance,[53] which holds that states, not private sector actors like the Internet Corporation for Assigned Names and

[47] *See* Anupam Chander, *The Asian Century?*, 44 U.C. Davis L. Rev. 717, 727 (2011) (noting the Five Principles for Peaceful Coexistence, including "mutual non-interference in each other's internal affairs").

[48] *See* Wang, *supra* note 43, at 397; Franz-Stefan Gady, *The Wuzhen Summit and the Battle Over Internet Governance*, Diplomat (Jan. 14, 2016), https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/; Bruce Sterling, *Respecting Chinese and Russian Cyber-Sovereignty in the Formerly Global Internet*, Wired (Dec. 22, 2015), https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in- the-formerly-global-internet/ [https://perma.cc/K743-B5VD] (archived Jan. 9, 2022).

[49] *See* Jacky Wong, *Didi and the Big Chill on China's Big Data*, Wall St. J. (July 5, 2021), https://www.wsj.com/articles/didi-and-the-big-chill-on-chinas-big-data-11625479452 (subscription required).

[50] *See* Li Qiaoyi & Hu Yuwei, *Chinese Regulator Orders App Stores to Remove Didi, Shows Resolve to Enhance Data Protection*, Global Times (July 4, 2021), https://www.globaltimes.cn/page/202107/1227778.shtml ("Ride-hailing firms manage large amounts of data regarding national transport infrastructure, flows of people and vehicles, among other types of information that involve national security, according to Dong. The rise of 'data sovereignty' versus the U.S. government's vigilance against Chinese firms ought to be a wake-up call for national security awareness to be given priority when it comes to fundraising plans in areas that might pose threats to China's national security, Dong told the Global Times on Sunday.").

[51] *See* Wang, *supra* note 43, at 397.

[52] *See id.* at 424 (explaining China views cybersecurity as another national security domain alongside land, sea, air, and space).

[53] *Id.* at 443–44.

Numbers (ICANN), should be driving Internet governance.[54] In contrast, the "bottom-up multi-stakeholderism" subscribed to by the United States and other Western countries[55] holds that the private sector and civil society should remain key players in Internet governance.[56] The Western "information freedom" approach to the Internet[57] is perceived as a threat to "Chinese ideological security" and a tool of cultural imperialism.[58] The Chinese government instead seeks to use the Internet to consolidate party control, maintain social order, and proliferate desirable Socialist and Confucian values such as " 'patriotism,' 'loyalty to the communist party,' 'dedication to one's work,' 'honesty,' [and] 'filial piety,' " to "develop a cohesive, Socialist nation."[59] President Xi affirmed this vision in 2016, stating, "we must . . . strengthen positive online propaganda, foster a positive, healthy, upward and benevolent online culture, use the Socialist core value view and the excellent civilizational achievements of humankind to nourish people's hearts and nourish society."[60]

China sees U.S. Internet infrastructure hegemony as a threat to its digital sovereignty.[61] In 2016, President Xi stated, "the fact that [the internet's] core technology is controlled by others is our greatest hidden danger."[62] Accordingly, the government has been investing heavily in research and development of Internet technology[63] and "territorializing critical infrastructure"[64] to escape Western technical and physical network dependence. Part of this effort has been a proliferation of Critical Information Infrastructure (CII) regulations,[65] including data localization regulations through the 2017 Cybersecurity Law (CSL).[66] Not only does Article 37 of the CSL require that data and personal information originating in China be stored within China,

[54] *See id.* (explaining that China opposes the current system where a U.S. corporation, ICANN (Internet Corporation for Assigned Names and Numbers), controls root ownership).
[55] *Id.* at 399.
[56] *See id.* at 444.
[57] *Id.* at 400.
[58] *Id.* at 406.
[59] *Id.* at 407.
[60] *Xi Jinping Gives Speech at Cybersecurity and Informatization Work Conference*, China Copyright & Media (Apr. 19, 2016), https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ [https://perma.cc/JH49-FMJM] (archived Jan. 9, 2022).
[61] *See* Wang, *supra* note 43, at 404–05 (explaining that China perceives U.S. corporate and civil society control over domain names and U.S.-made infrastructure as favoring U.S. interests).
[62] *Id.* at 405.
[63] *See id.* at 434, 436.
[64] *Id.* at 435.
[65] *See id.* at 436–37.
[66] *See id.* at 408, 456.

but CII operators must also undergo "security assessments" before that data can be transferred abroad.[67] (The first such security assessment—against the ride-hailing company Didi—is described below.)

Content regulation and censorship is another integral component of China's "information sovereignty" on the Internet.[68] Though China's approach to content regulation is more extreme than in other countries,[69] it rejects accusations that its cyber sovereignty policies simply mask authoritarian control.[70] Instead, the government claims to censor "subversive," "harmful," "obscene," or "malicious" content while welcoming "kind criticism."[71] Content control remains a clear goal. In 2017, the Cyber Administration of China (CAC) asserted that "Online positive publicity must become bigger and stronger, so that the Party's ideas always become the strongest voice in cyberspace."[72] The Theoretical Studies Center Group of CAC also commented in the Communist Party magazine Qiushi that "[w]e must . . . steadily control all kinds of major public opinion; dare to grasp, dare to control, and dare to wield the bright sword; refute erroneous ideas in a timely manner" to "prevent mass incidents and public opinion from becoming online ideological patterns and issues."[73]

Some of the measures China takes to regulate content and maintain a "clear cyberspace"[74] include blocking virtual private network (VPN) access, algorithms that divert searches, the Real Name Registration Policy,[75]

[67] *See id.* at 456–57; Willem Gravett, *Digital Neo-Colonialism: The Chinese Model of Internet Sovereignty in Africa*, 20 Afr. Hum. Rts. L.J. 125, 130 (2020) (data on Chinese users must be hosted on Chinese mainland); *Cross-Border Data Transfers: CSL vs. GDPR*, Reed Smith (Jan. 2, 2018), https://www.reedsmith.com/en/perspectives/2018/01/cross-border-data-transfer-csl-vs-gdpr [https://perma.cc/HXT2-73TD] (archived Jan. 9, 2022); Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, Lawfare Blog (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/2GWM-VYST] (archived Jan. 9, 2022).

[68] *See* Wang, *supra* note 43, at 452.

[69] *See id.* at 466.

[70] *See id.* at 416.

[71] *Id.* at 422. President Xi commented that "to build a well-functioned Internet public sphere is not to censor all negative comments and only endorse a single perspective; it is to welcome, investigate, and learn lessons from the kind criticism but reject those comments which turn things upside down, mix the black with the white, spread rumors with malicious intentions, commit crimes and override the Constitution." *Id.* at 416.

[72] Elsa Kania, Samm Sacks, Paul Triolo, & Graham Webster, *China's Strategic Thinking on Building Power in Cyberspace*, New Am. (Sept. 25, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace; Wang, *supra* note 43, at 453; Gravett, *supra* note 67, at 131.

[73] Wang, note 43, at 455–56.

[74] *Id.* at 455.

[75] *Id.* at 456; Gravett, *supra* note 67, at 130 (describing a 2017 law that makes social media companies register users with their real names).

and making domain name service providers responsible for content by their clients through a 2017 update to Article 28 of the Measures for the Administration of Internet Domain Names Law.[76] However, standards for what information is "erroneous" or in violation of the law remain unclear.[77] The government also introduced an "Interview Mechanism," which functions as a warning to websites and companies hosting prohibited content before sanctions, fines, or criminal prosecutions are pursued.[78] Such interviews incentivize self-correction and willing removal of censored content by allowing websites to stay up and avoid fines or harsher penalties like closure.[79]

Through its "Digital Silk Road," which adopts one of the authors' framing of the Internet as the "Electronic Silk Road,"[80] China has sought to advance its digital trade connections with developing countries across the world. This part of China's Belt and Road Initiative promotes collaboration between China and developing countries in critical Internet infrastructure projects, e-commerce, and artificial intelligence (AI).[81] By increasing developing African and Eurasian nations' Internet access,[82] as well as their dependence on Chinese technology, China acquires soft power while creating new markets for Chinese technology exports and e-commerce.[83] Many Western governments have expressed concern that China's grip on developing nations' Internet infrastructure could leave them vulnerable to possible surveillance by either China or local governments.[84] Thus, even as the Chinese government worries about foreign influences via the Internet, many other governments worry about the Chinese government exerting its influence via the Internet. China looms especially large in the geopolitics that are driving many assertions of digital sovereignty.

[76] *See* Wang, note 43, at 457–58.
[77] *See id.*
[78] *See id.* at 459–61, 464.
[79] *See id.* at 460–61, 464.
[80] Anupam Chander, The Electronic Silk Road (2013).
[81] *See* Wang, *supra* note 43, at 441.
[82] *See id.* at 416–17.
[83] *See id.* at 447; Gravett, *supra* note 67, at 131 (international consensus building).
[84] *See* Wang, *supra* note 43, at 441–42.

B. The EU: Embracing Digital Sovereignty

Nowhere have calls for digital sovereignty been more intense than in Europe. As early as 2006, President Jacques Chirac of France called on Europeans to develop an indigenous information search capacity to respond to "the global challenge posed by Google and Yahoo."[85] As early as 2010, the French government was sounding the alarm about the loss of sovereignty in the face of foreign technology firms. François Fillon, then prime minister, observed that with respect to cloud computing, "North Americans dominate this market, which nevertheless constitutes an absolutely major stake for the competitiveness of our economies, for sustainable development and even, I dare say it, for the sovereignty of our countries."[86] Among the strategies the government adopted was the promotion of "*le cloud souverain*"—the "sovereign cloud"—through partnerships with cloud computing enterprises to support domestic employment, among other goals.[87] In 2013, the French government detailed efforts to "build a France of digital sovereignty," including the desire to make to "make France the world leader" in the field of "Big Data."[88]

EU digital sovereignty has been expressed perhaps most fully through a robust assertion of data protection law. The EU's data protection law covers not only companies based in the EU but also foreign companies that target

[85] Chander, *supra* note 80, at 40.

[86] Pierre Noro, *Le Cloud Souverain Est De Retour: Généalogie D'une Ambition Emblématique De La Souveraineté Numérique En France*, SciencesPo: Chaire Digital, Gouvernance et Souveraineté (July 20, 2020), https://www.sciencespo.fr/public/chaire-numerique/2020/07/20/cloud-souverain-genealogie-ambition-emblematique-souverainete-numerique/ (speech by Prime Minister François Fillon on broadband and the digital economy, Jan. 18, 2010).

[87] The French government then invested in two French cloud projects. *See* Delphine Cuny, *"Cloud" à la Française: Fleur Pellerin Justifie les Deux Projets Concurrents*, La Tribune (Oct. 2, 2012), https://www.latribune.fr/technos-medias/informatique/20121002trib000722485/cloud-a-la-francaise-fleur-pellerin-justifie-les-deux-projets-concurrents.html. Germany too has pursued a similar data sovereignty strategy by establishing local cloud centers for the storage of government information. *See* Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 Yale J.L. & Tech. 182, 189 (2017).

[88] *See* MINISTÈRE DU REDRESSEMENT PRODUCTIF [MINISTRY OF ECON. REGENERATION], THE NEW FACE OF INDUSTRY IN FRANCE 51 (2013), available at https://www.economie.gouv.fr/files/nouvelle_france_industrielle_english.pdf [hereinafter NEW FACE OF INDUSTRY] (cited in Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 690–91 (2015)). President François Hollande announced the national innovation program on September 12, 2013, with a plan that used the term "sovereignty" no less than a dozen times. *See* Nicholas Vinocur, *Hollande Turns to Robots, Driverless Cars to Revive French Industry*, Reuters (Sept. 12, 2013), https://www.reuters.com/article/france-industry/hollande-turns-to-robots-driverless-cars-to-revive-french-industry-idUSL5N0H73T020130912.

EU residents and process information about them. This extraterritorial application of law has made the EU into an Internet-regulatory superpower.[89]

The German government announced in July 2020 that it would "establish digital sovereignty as a leitmotiv of European digital policy."[90] The European Commission similarly declared its intention to "strengthen its digital sovereignty and set standards, rather than following those of others."[91]

C. Russia: Promoting the Runet

Russia has embraced digital sovereignty as official policy, even seeking to create an entirely separable Russian Internet, dubbed the "Runet." This reflects a u-turn in policy from early years when the Russian government embraced the Internet as a means to transform the country from reliance on natural resources. In the wake of the Arab Spring, the Russian government began to assert greater control of the Internet, recognizing the Internet's demonstrated potential to help bring down governments.[92] Today, Russia's official policy is to create a "sovereign Runet"—a Russian Internet where the Russian government exercises "more control over what its citizens can access."[93] In 2019, Vladimir Putin signed a "Sovereign Internet" bill into law, gaining broad powers to monitor and control traffic on the Russian Internet through hardware and software controls installed in Russian telecommunications infrastructure and even to restrict the global Internet in certain

[89] Anu Bradford, The Brussels Effect: How the European Union Rules the World (2020) (noting that "the EU remains an influential superpower that shapes the world in its image"); Anupam Chander, Margot E. Kaminski, & William McGeveran, *Catalyzing Privacy*, 105 Minn. L. Rev. 1733, 1734 (2021) (explaining that the GDPR's effectuation "positioned the European Union as the world's privacy champion.").

[90] Together for Europe's Recovery, Programme for Germany's Presidency of the Council of the EU 2020 8 (2020), available at https://www.eu2020.de/blob/2360248/978a43ce17c65efa8f506c2a484c8f2c/pdf-programm-en-data.pdf.

[91] *A Europe Fit for the Digital* Age, Eur. Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (last visited Jan. 15, 2022) [https://perma.cc/RJ6Z-FKB7] (archived Jan. 15, 2022). The German Presidency of the EU Council declared in 2020, "Europe must bolster its digital sovereignty to effectively respond to future challenges, guarantee livelihoods and ensure the security of its citizens." *See Expanding the EU's Digital Sovereignty*, EU2020, https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828 (last visited Jan. 14, 2022).

[92] *See* Alexandra V. Orlova, *"Digital Sovereignty," Anonymity and Freedom of Expression: Russia's Fight to Re-Shape Internet Governance*, 26 U.C. Davis J. Int'l L. & Pol'y 225, 228 (2020).

[93] *See* Jane Wakefield, *Russia "Successfully Tests" Its Unplugged Internet*, BBC News (Dec. 24, 2019), https://www.bbc.com/news/technology-50902496 [https://perma.cc/QK3E-2668] (archived Jan. 9, 2022) (quoting Professor Alan Woodward as saying that the Runet would keep Russian citizens "within their own bubble").

cases.[94] Ironically, given prolific Russian interventions in elections abroad, Russian demands for a sovereign Internet are driven in part by claims of "information warfare" waged by Western countries against the Russian government.[95] One of the goals of the Runet is to protect the Russian internet from "external negative influences."[96]

Russia employs a common and highly controversial tactic for implementing digital sovereignty: data localization.[97] Law No. 242-FZ, which came into effect in 2015, requires data operators to ensure that the recording, systematization, accumulation, storage, update/amendment, and retrieval of personal data of citizens of the Russian Federation are made using databases located in the Russian Federation.[98] In 2015, a Russian court blocked LinkedIn from the country for failure to localize data. In 2020, Russian regulators fined Facebook, Google, and Twitter for refusing to store their data in Russia, with Facebook paying the $53,000 penalty in 2021.[99] In 2021, Russia's Internet regulator Roskomnadzor throttled traffic to Twitter after Twitter failed to delete posts urging children to take part in anti-government protests.[100] Roskomnadzor has also threatened to throttle Google's traffic if it refuses to localize data.[101]

[94] *See* Ksenia Koroleva, Ulrich Wuermeling, & Tim Wybitul, *RuNet Law Comes into Force: What Is Next*, JDSupra (Nov. 27, 2019), https://www.jdsupra.com/legalnews/runet-law-comes-into-force-what-is-next-72937/.

[95] Orlova, *supra* note 92, at 231.

[96] *See The Ministry of Telecom and Mass Communications: Government Agencies and Telecom Operators Are Ready to Ensure Stable Operation of the Runet*, TASS (Dec. 23, 2019), https://tass.ru/ekonomika/7407631.

[97] For an argument that data localization both undermines domestic development and increases the power of local authoritarians, *see generally* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015).

[98] *See* Federal'nyy zakon No. 242-FZ ot 21 iyulya 2014 g. O vnesenii izmeneniy v nekotoryye zakonodatel'nyye akty Rossiyskoy Federatsii v chasti, kasayushcheysya obnovleniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh [Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks], FEDERAL'NYY ZAKON [FZ] [Federal Law] 2014, No. 242-FZ, art. 18 § 5.

[99] *See* Adrian Shahbaz, Allie Funk, & Andrea Hackl, *Special Report 2020: User Privacy or Cyber Sovereignty?*, Freedom House, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty (last visited Jan. 14, 2022); *Facebook Pays Russia $50K Fine For Not Localizing User Data*, Moscow Times (Nov. 26, 2020), https://www.themoscowtimes.com/2020/11/26/facebook-pays-russia-50k-fine-for-not-localizing-user-data-a72152.

[100] *See* Madeline Roache, *How Russia Is Stepping Up Its Campaign to Control the Internet*, Time (Apr. 1, 2021), https://time.com/5951834/russia-control-internet/.

[101] *See Roskomnadzor Orders Twitter and Facebook to Localize Russian Users' Data by July 1*, Meduza (May 26, 2021), https://meduza.io/en/news/2021/05/26/roskomnadzor-orders-twitter-and-facebook-to-localize-russian-users-data-by-july-1.

Russia has domestic versions of key Internet tools, including a browser, cloud computing service, maps, search engine, messaging service, and two social networks, most of which are owned by the Russian companies Yandex and Mail.ru. An antitrust case brought by Yandex against Google had ended with the requirement that Russians could choose Yandex's search engine on Android devices. Local alternatives to foreign apps reduce the costs of blocking those foreign apps. In 2022, rather than seeking the support of international authorities to clamp down on information online about its invasion of Ukraine, Russia turned to its domestic internet controls. In March 2022, the Russian Internet regulator, Roskomnadzor blocked access to Facebook on grounds that it discriminated against Russia, including by blocking RT and Sputnik across the European Union. A Russian court upheld the ban, concluding that Meta was carrying out extremist activities, though it exempted Meta's WhatsApp "due to its lack of functionality for the public dissemination of information." Shortly thereafter, Russia blocked Google News for linking to information that it considered "inauthentic" about the Ukraine invasion.

D. The United States: Digital Sovereignty by Default

One nation is more likely to criticize digital sovereignty than to explicitly embrace it: the United States.[102] This is because the United States is in the unique position of being home to many of the world's leading technology firms. This means that during the ordinary course of regulating its companies, the United States exercised digital sovereignty from the start. The U.S. FTC, for example, cited GeoCities for privacy failures as early as 1998.[103] There was never a moment when the United States did not exercise digital sovereignty,

[102] *See* Stephane Couture & Sophie Toupin, *What Does the Notion of "Sovereignty" Mean When Referring to the Digital?*, 21 NEW MEDIA & SOC'Y 2305, 2313 (2019) ("Within the United States, digital sovereignty (or related terms) usually have negative connotations across the political spectrum."). For example, the U.S. Ambassador to the European Union, Anthony Gardner, cautioned the EU in 2015: "The calls from some Member States, however, to promote so-called digital sovereignty, discriminatory regulation, or forced data localization will not help Europe to maintain and extend its leadership in the global digital economy." *See Remarks for TABC Conference: Perspectives on the EU's Digital Single Market Strategy – The Transatlantic Perspective*, U.S. MISSION TO THE EUROPEAN UNION (Sept. 15, 2015), https://useu.usmission.gov/remarks-tabc-conference-perspectives-eus-digital-single-market-strategy-transatlantic-perspective-2/.

[103] *FTC, GeoCities Settle on Privacy*, CNET (Aug. 13, 1998), https://www.cnet.com/tech/services-and-software/ftc-geocities-settle-on-privacy/; GeoCities, 127 F.T.C. 94 (1999).

and thus the United States never had to go out of its way to assert it: it was a natural consequence of the geography of the Internet.[104]

The dominance of American technology firms does not mean that the United States has not faced controversies along the way. The first Digital Millennium Copyright Act prosecution was strikingly brought against a Russian, who happened to be visiting the United States for the Def Con conference in 2002.[105] The United States accused the Russian programmer of selling tools that broke through Adobe's e-book security. Jennifer Granick, a leading digital rights advocate, argued at the time that the United States should not impose its interpretation of copyright law on foreign nations.[106]

The U.S. government has routinely seized domain names of sites that violate domestic law in part because top-level domain names are indexed on a domain name server in Virginia. Karen Kopel, writing in a student note in 2013, observed:

> Since its inception over two and a half years ago, [US federal] Operation In Our Sites has seized 1,719 domain names of which over 690 have been forfeited, ranging from websites selling allegedly counterfeit luxury goods, sports memorabilia, and pharmaceuticals, to websites that host copyrighted music, movies, TV shows, software, and websites that only link to this content.[107]

But these enforcement actions, Kopel suggests, lack sufficient process and may infringe on free speech concerns.[108]

The fact that the largest Internet companies are based in the United States also means that data about Americans are typically stored in the United States. This allows prosecutors to use traditional judicial processes within

[104] Anupam Chander, *Law and the Geography of Cyberspace*, 6 W.I.P.O.J. 99, 101–02 (2014).

[105] *See generally* United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002); Robert Lemos, *Russian Crypto Expert Arrested at Def Con*, CNET (Mar. 2, 2002), https://www.cnet.com/news/russian-crypto-expert-arrested-at-def-con/. The DMCA criminalizes the sale of tools that break encryption protecting copyrighted works, such as DVDs and e-books.

[106] *See* Matt Richtel, *Russian Company Cleared of Illegal Software Sales*, N.Y. Times (Dec. 18, 2002), https://www.nytimes.com/2002/12/18/business/technology-russian-company-cleared-of-illegal-software-sales.html [https://perma.cc/S6NB-WJKF] (archived Jan. 9, 2022) (quoting Jennifer Granick as saying that the acquittal of the Russian company in the case was "good for democracy: people in other countries can make determinations about what is right and wrong for themselves.").

[107] Karen Kopel, *Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice*, 28 Berkeley Tech. L.J.859, 860 (2013).

[108] *Id*. at 885–93.

the country to access the data, subject to Fourth Amendment and statutory protections. But when U.S. prosecutors sought information stored in Ireland on Microsoft servers, Microsoft protested that this was beyond the statutory authority of prosecutors.[109] Congress intervened to amend the law to grant authority to prosecutors to use judicial process to require companies to produce data held abroad.[110]

But earlier enforcement efforts against Internet enterprises do not seem to compare with the regulatory demands that resound today across the political spectrum in the United States. If there ever was a laissez-faire era for U.S. Internet regulation,[111] that era is distinctly over.[112]

At the same time, the U.S. government remains concerned that foreign efforts to assert digital sovereignty can be a guise for old-fashioned protectionism. For example, the U.S. government's 2021 report on "foreign trade barriers" cites EU digital sovereignty practices as possibly "unfairly target[ing] large U.S. service suppliers and hamper[ing] their ability to provide innovative, Internet-based services in the EU."[113]

E. The Global South: Avoiding Data Colonialism

Even as access to the Internet has grown dramatically,[114] many governments in the Global South worry about being left behind in the digital economy. Digitization, whether led by foreign or domestic firms, has, of course, proven critical to their economic growth, giving individuals information about markets and opportunities that was hard to obtain previously. Yet, foreign companies have an outsized presence in their digital lives. Developing nations fear recapitulating colonialism, specifically, of being both the raw

[109] *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 204–05 (2d Cir. 2016).

[110] USA CLOUD Act, 18 U.S.C. § 2713, *et seq.* (2012).

[111] For a comparative history of U.S. Internet regulation, *see generally* Anupam Chander, *How Law Made Silicon Valley*, 63 Emory L.J. 639 (2014).

[112] *See* John Cassidy, *Will Joe Biden and Lina Khan Cut the Tech Giants Down to Size?*, New Yorker (June 21, 2021), https://www.newyorker.com/news/our-columnists/will-joe-biden-and-lina-khan-cut-the-tech-giants-down-to-size.

[113] U.S. Trade Representative, 2021 National Trade Estimate Report on Foreign Trade Barriers 216 (2021).

[114] About half of the world's people now have Internet access. *Individuals Using the Internet*, World Bank, https://data.worldbank.org/indicator/IT.NET.USER.ZS.

materials (now in the form of data) and markets for Western manufacture (in the form of processed information).[115]

In 2021, South Africa published a draft "National Data and Cloud Policy" that explicitly seeks to "promote South Africa's data sovereignty."[116] The draft policy laments that "data generated in Africa and South Africa is mostly stored in foreign lands and, where stored locally, is owned by international technology giant companies."[117] It seeks to reverse that through a data localization mandate: "All data classified/identified as critical Information Infrastructure shall be processed and stored within the borders of South Africa."[118] The draft policy also announces, "[d]ata generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled."

In fact, in its recently released "Digital Transformation Strategy for Africa (2020–2030)," the African Union envisions "data sovereignty" as one of its policy priorities.[119] It, too, suggests data localization as a strategy to promote data sovereignty: "Even though Africa is at the moment less restrictive, soon it will be necessary to ensure localization of all personal data of Africa's citizens."[120] In Senegal, President Macky Sall hopes to "guarantee[] Senegalese digital sovereignty" by building a data center within the country with the help of a Chinese loan and Huawei equipment and technical assistance.[121] This is part of China's Digital Silk Road effort, tying countries to China through technology.

After Twitter deleted a tweet by President Muhammadu Buhari that some saw as threatening violent reprisal against protestors, the Nigerian government simply banned Twitter from the country.[122] In the battle between

[115] *See* Angelina Fisher & Thomas Streinz, *Confronting Data Inequality*, 60 Colum. J. Transnat'l L. 829, 831 (2022).

[116] South Africa Dept. of Comm. & Digital Tech., Invitation to Submit Written Comments on the Proposed National Data and Cloud Policy 11, Apr. 1, 2021.

[117] *See Data Generated in SA Is the Property of SA, Says New Draft Govt Policy – And Cops Need Access*, Bus. Insider SA (Apr. 6, 2021), https://www.businessinsider.co.za/a-draft-national-data-and-cloud-policy-demands-data-sovereignty-for-south-africa-2021-4.

[118] South Africa Dept. of Comm. & Digital Tech., *supra* note 116, at 27.

[119] The Digital Transformation Strategy For Africa (2020–2030), African Union 11 (2020), https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

[120] *Id.*; *see* Halefom H. Abraha, *How African Countries Can Benefit From the Emerging Reform Initiatives of Cross-border Access to Electronic Evidence*, Cross-Border Data Forum (July 6, 2020), https://www.crossborderdataforum.org/how-african-countries-can-benefit-from-the-emerging-reform-initiatives-of-cross-border-access-to-electronic-evidence/.

[121] Dan Swinhoe, *Senegal to Migrate All Government Data and Applications to New Government Data Center*, Data Ctr. Dynamics (June 23, 2021), https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/.

[122] *Nigerian Govt Accuses Twitter of Double Standards, Supporting Secessionists*, Bus. Standard (June 3, 2021), https://www.business-standard.com/article/international/nigerian-govt-accu

developing states and big tech, Nigeria shows that a government willing to forgo a platform that it or its citizens use can still win. In the non-Western parts of the world (including both developing countries and the former Soviet Bloc nations), assertions of digital sovereignty are more likely to include shutdowns of a website or even the Internet. Governments may be more likely to turn to complete shutdowns of a site or even the Internet generally (through disabling cell services) if they feel that a foreign platform will not otherwise comply with its censorship demands.

Indigenous peoples are also seeking digital sovereignty. Indigenous data sovereignty "deals with the right and ability of tribes to develop their own systems for gathering and using data and to influence the collection of data by external actors."[123] For example, the Māori Data Sovereignty Network seeks to ensure that Māori peoples have sovereignty over the "data produced by Māori or that is about Māori and the environments we [the Māori] have relationships with."[124]

III. How Digital Sovereignty Is Different

Digital sovereignty is not merely the assertion of sovereignty online. The last few decades have taught us that the Internet changes the nature of sovereignty in a variety of ways. First, because of the global nature of the Internet, digital sovereignty almost always has global implications, whether it involves speech regulation, privacy, consumer protection, competition concerns, or law enforcement; thus, digital sovereignty can create significant roadblocks to one of the Internet's key virtues—its empowering of global connections. Second, because the digital sphere is intermediated by corporations, the

ses-twitter-of-double-standards-supporting-secessionists-121060300481_1.html. The tweet in question stated: "Many of those misbehaving today are too young to be aware of the destruction and loss of lives that occurred during the Nigeria civil war. Those of us in the fields for 30 months, who went through the war, will treat them in the language they understand," the president tweeted on Tuesday night." *Id*.

[123] Christopher B. Chaney, *Data Sovereignty and the Tribal Law and Order Act*, 65-APR FED. LAW. 22, 23 (2018); *see also* Aila Hoss, *Exploring Legal Issues in Tribal Public Health Data and Surveillance*, 44 S. ILL. U. L.J. 27, 38 (2019); Rebecca Tsosie, *Tribal Data Governance and Informational Privacy: Constructing "Indigenous Data Sovereignty"*, 80 MONT. L. REV. 229, 229–30 (2019) ("Data sovereignty describes the right of a nation to 'govern the collection, ownership and application of data' concerning the tribe or its members and to control data that is housed within tribal territory.").

[124] Lida Ayoubi, *Intellectual Property Commercialisation and Protection of Mātauranga Māori in New Zealand Universities*, 28 N.Z. U. L. REV. 521, 553 (2019).

assertion of digital sovereignty typically occurs vis-à-vis corporations, not governments. Third, because daily life is increasingly permeated by the Internet, digital sovereignty can offer governments surveillance tools that far exceed any history has previously provided. Fourth, because of the dominance of U.S .technology companies globally, governments can readily weaponize digital sovereignty to serve protectionist goals.

A. Always Global

Unless one cuts off the local Internet from the global Internet (a possibility that China, Iran, North Korea, and Russia are working toward in different measures), the regulation of the Internet almost inevitably involves foreign actors.[125] Consider a French court's order to Yahoo! in 2000 to stop permitting French residents to access Nazi materials. Yahoo! responded by banning these materials across the world.[126] The EU's General Data Protection Regulation (GDPR) does not regulate the processing of personal information about a US person in a transaction in the United States, but yet Microsoft and numerous other companies have chosen to apply at least parts of the GDPR to their practices worldwide.[127] Anu Bradford labels this the "Brussels Effect."[128] While David Johnson and David Post famously argued that the global nature of the Internet made any sovereign assertion illegitimate,[129] Jack Goldsmith demonstrated that inter-jurisdictional conflicts

[125] *Cf.* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 185 (2018) (observing "the transnational nature of both data and the companies that regulate our data"). Jennifer Daskal argues that the differences "between data and its tangible counterpart," in particular, data's mobility, interconnectedness, and divisibility, demonstrate the difficulties of applying traditional jurisdictional frameworks to internet problems. Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 365–78 (2015).

[126] Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme, 433 F.3d 1199, 1205 (9th Cir. 2006) (Fletcher, J.) ("Yahoo's new policy eliminates much of the conduct prohibited by the French orders.").

[127] *See* Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT ON THE ISSUES (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ [https://perma.cc/SV9F-U9M9] (archived Jan. 9, 2022) ("we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide").

[128] Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3 (2012) ("Unilateral regulatory globalization occurs when a single state is able to externalize its laws and regulations outside its borders through market mechanisms, resulting in the globalization of standards.").

[129] *See* David R. Johnson & David Post, *Law and Borders-the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) ("Territorial regulation of online activities serves neither the legitimacy nor the notice justifications. There is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group.").

are not new with the Internet and that international law has tools to manage them.[130] Paul Berman goes further to argue that pluralist approaches to governance should be normatively welcome as they better express contemporary conditions.[131]

Digital sovereignty increasingly means regulating not only one's citizens alone but also foreigners—typically firms offering services across the world. In order for law to be meaningful in a world of Internet globalization, states must regulate foreign entities. It is this necessarily extraterritorial[132] exercise of jurisdiction that increases the difficulty, complexity, and risk of digital sovereignty.

At the same time, excessive assertions of digital sovereignty can tear the Internet apart, relegating all to national spaces for commerce and speech, where once individuals could transact and speak with each other across the world. The specter of the 193 nations of the United Nations—and other sub- and supra-national jurisdictions as well—regulating the internet at the same time seems daunting indeed. Instead of being the world's most-free-speech zone, the Internet may become the world's most-unfree zone, merely a conglomeration of the censorship and rules of all the jurisdictions in the world.

B. Against Corporations

Where sovereignty has historically been asserted in relation to foreign states, digital sovereignty is equally or perhaps more likely to be asserted against foreign corporations. Foreign corporations are the ones that are dealing directly with their residents—collecting data, offering services, and moderating speech. Jennifer Daskal observes that much of transnational Internet governance "is largely being mediated by the private parties that hold and manage our data."[133] She writes, "It is these companies that increasingly determine whose rules govern and, in key ways, how they are interpreted and applied."[134] Writing about digital sovereignty, Lucien Floridi observes, "The most visible clash is between companies and states."[135]

[130] *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).
[131] *See* Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 490 (2002).
[132] The application of the term "extraterritorial" is itself open to debate, as some would argue that the exercise of jurisdiction against companies located abroad that are operating in one's jurisdiction is in fact an exercise simply of territorial jurisdiction.
[133] Daskal, *supra* note 125, at 185.
[134] *Id.*
[135] *See* Floridi, *supra* note30, at 371.

Indeed, the European Parliament's study of digital sovereignty explicitly rests its call for digital sovereignty on this ground: "Strong concerns have been raised over the economic and social influence of non-EU technology companies, which threatens EU citizens' control over their personal data, and constrains both the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws."[136] Much of the enforcement activity under the GDPR is, accordingly, targeted at corporations. Much as some U.S. residents worry about the exploitation of their data by U.S. companies, India worries that foreign companies are benefiting from local data—the 21st-century version of serving as the source of raw materials for the manufacturers of the Global North.[137]

C. More Control

As Neil Richards observes, "[we] are living in an age of surveillance. The same digital technologies that have revolutionized our daily lives over the past three decades have also created ever more detailed records about those lives."[138] Those digital technologies can be utilized by the state. Michael Birnhack and Niva Elkin-Koren worry about what they called "the invisible handshake" between the government and corporations: "Whether the Big Brother we distrust is government and its agencies, or multinational corporations, the emerging collaboration between the two in the online environment produces the ultimate threat."[139]

In *Seeing Like a State*, historian James C. Scott argues that increases in what he calls "legibility" (the ability of the state to better understand its population) were a critical part of large governmental projects.[140] Scott sees this legibility, when combined with hubris, as leading to failed schemes—but increases in legibility could also lead to greater control. The digital world

[136] *See* Eur. Parliamentary Res. Serv., Digital Sovereignty for Europe 1 (2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

[137] *Mukesh Ambani Says "Data Colonisation" as Bad as Physical Dolonisation*, Econ. Times (Dec. 19, 2018), https://economictimes.indiatimes.com/news/company/corporate-trends/mukesh-ambani-says-data-colonisation-as-bad-as-physical-colonisation/articleshow/67164810.cms?utm_source%3Dtwitter_web%26utm_medium%3Dsocial%26utm_campaign%3Dsocialsharebuttons.

[138] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1936 (2013).

[139] Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 Va. J.L. & Tech. 6, 3 (2003).

[140] *See generally* James C. Scott, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed (1998).

enlarges governmental legibility dramatically, even more so when the government gains access to information collected by private companies. The legibility that Internet companies seek into their users for commercial purposes, which Julie Cohen observes,[141] can be exploited by the state as well.

Scott argues that mid-20th-century failures of government planning resulted from hubris, with the planners "forgetting that they were mortals and acting as if they were gods."[142] For Scott, the absence of representative institutions reduces resistance to these large planning measures. Scott's government planners were largely well-intentioned, with noble goals of a more egalitarian society.[143] We should be mindful that digital regulators, whether well-intentioned or not, should not wield unchecked power. This will require both a vigorous civil society and laws that are designed with appropriate checks for governmental abuse.

D. Enables Protectionism

When President of the European Commission Jean-Claude Juncker proposed the "Digital Single Market" policy in 2015, he focused on promoting European innovation—but not through protectionist applications of regulation: "Today, we lay the groundwork for Europe's digital future. I want to see pan-continental telecom networks, digital services that cross borders, and a wave of innovative European start-ups."[144] Günther Oettinger, then a member of the European Commission for Budget and Human Resources, explained that "[t]he digital single market can be a win-win" for both European and Silicon Valley firms.[145] Andrus Ansip, the European Commissioner for Digital Single Market from 2014 to 2019, similarly suggested, "[t]he digital single market will provide opportunities for trade, investment, innovation

[141] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 38 (2019).

[142] Scott, *supra* note 52, at 342.

[143] *Id.* at 346.

[144] Hamza Shaban, *European Union Unveils Digital Single Market Plan*, Buzzfeed News (May 6, 2015), https://www.buzzfeednews.com/article/hamzashaban/european-union-unveils-digital-single-market-plan; *see* David O'Sullivan, *Stop the Hysteria: Of Course, Europe Wants an Open Internet*, Wired (Apr. 30 2015), https://www.wired.com/2015/04/eu-ambassador-on-open-internet/.

[145] Hamza Shaban, *EU Digital Commission to Silicon Valley: Relax*, Buzzfeed News (Sept. 25, 2015), https://www.buzzfeednews.com/article/hamzashaban/eu-digital-commissioner-to-silicon-valley-relax.

not only for Europe, but globally—also, for the United States."[146] Fredrik Persson, chairman of the Confederation of Swedish Enterprise cautioned that European efforts toward digital sovereignty "should not create a European fortress that pulls up the drawbridge to the outside world."[147] In March 2021, German Chancellor Angela Merkel, Danish Prime Minister Mette Frederiksen, Estonian Prime Minister Kaja Kallas, and Finnish Prime Minister Sanna Marin sent a joint letter to European Commission President Ursula von der Leyen encouraging European efforts for digital sovereignty but cautioning that the EU should avoid protectionist strategies to build digital sovereignty: "Digital sovereignty is about building on our strengths and reducing our strategic weaknesses, not about excluding others or taking a protectionist approach."[148] Many European leaders have explicitly disavowed protectionism, instead embracing the coexistence of foreign and domestic technology companies.

Other voices within the EU, however, portray issues of digital sovereignty as a zero-sum geopolitical struggle. In 2019, French President Emmanuel Macron declared, "[t]he battle we're fighting is one of sovereignty." He continued, "[i]f we don't build our own champions in all new areas—digital, artificial intelligence—our choices . . . will be dictated by others."[149] The European Parliament's study of digital sovereignty echoes this: "EU policymakers have identified a potential dependence on foreign technology as presenting a risk to Europe's influence."[150]

The European Parliament's study goes on to argue that the dominance of foreign Internet platforms in the EU is itself a hallmark of the loss of European sovereignty. The study explains: "[L]arge online platforms (mostly non-EU based) are increasingly seen as dominating entire sectors of the EU economy and depriving EU Member States of their sovereignty in areas such

[146] Hamza Shaban, *Digital Single Market Isn't Anti-American, Says EU Commissioner*, Buzzfeed News (May 28, 2015), https://www.buzzfeednews.com/article/hamzashaban/digital-single-market-isnt-anti-american-says-eu-commissione.

[147] Christakis, *supra* note 26, at 58.

[148] *See Estonia, EU countries propose faster 'European digital sovereignty'*, ERR News (Feb. 3, 2021), https://news.err.ee/1608127618/estonia-eu-countries-propose-faster-european-digital-sovereignty.

[149] Kenneth Propp, *Waving the flag of digital sovereignty*, Atlantic Council (Dec. 11, 2019), https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/ . It might be noted that this concern about too-powerful-foreign-corporations is uncomfortably coupled with the hope that these national champions will themselves be globally successful.

[150] Eur. Parliamentary Res. Serv., Digital Sovereignty for Europe 1 (2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

as copyright, data protection, taxation or transportation." But this argument seems misplaced. It is like arguing that because people drive Toyota cars on U.S. roads, Americans no longer control their streets. As long as the cars are regulated by local law, the fact that they might be built abroad should not undermine sovereignty.

Some see a zero-sum game with respect to the Internet with winners and losers. In 2020, Thierry Breton, the European Union's Commissioner for Internal Market, expressed confidence that EU companies would beat their American counterparts: "The winners of today will not be the winners of tomorrow."[151] At times, however, the European approach to digital sovereignty seems to be focused on replacing U.S. enterprises with European ones, a classic protectionist strategy. Commissioner Breton seeks to ensure that "European data will be used for European companies in priority, for us to create value in Europe."[152]

Even while seeking to rein in the power of U.S. tech titans, some in the EU seem to covet their own. In June 2021, "French President Emmanuel Macron announced the objective of having '10 companies worth €100 billion by 2030' in Europe . . . after he received . . . recommendations to encourage the emergence of digital giants in Europe."[153] Some in the EU wish to create their own "European digital champions."[154] Regulatory actions in the digital space are especially amenable to protectionist use because the largest players in the industry are often foreign-owned corporations. Whether justified or not, some saw Facebook's hand in the Trump administration's targeting of largely Chinese-owned TikTok.[155]

[151] Foo Yun Chee, *This Is the EU's Plan to Compete with Silicon Valley*, World Econ. F. (Feb. 20, 2020), https://www.weforum.org/agenda/2020/02/eu-data-market-technology-silicon-valley.

[152] Frances Burwell & Kenneth Propp, The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? 6 (2020).

[153] *See* Mathieu Pollet, *Macron Wants Europe to Have 10 Tech Giants Worth €100 Billion by 2030*, EURACTIV (June 16, 2021), https://www.euractiv.com/section/digital/news/macron-wants-europe-to-have-10-tech-giants-worth-e100-billion-by-2030/.

[154] *See* Theodore Christakis, "European Digital Sovereignty": Successfully Navigating between the "Brussels Effect" and Europe's Quest for Strategic Autonomy 89 (Dec. 2020) (e-book published by the Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.

[155] Georgia Wells, Jeff Horwitz, & Aruna Viswanatha, *Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok*, Wall St. J. (Aug. 23, 2020), https://www.wsj.com/articles/facebook-ceo-mark-zuckerberg-stoked-washingtons-fears-about-tiktok-11598223133#:~:text=Zuckerberg%20told%20Georgetown%20students%20that,American%20values%20and%20technological%20supremacy.

IV. Digital Sovereignty and the Russian Invasion of Ukraine

We can see the critical role of digital sovereignty by examining the digital battle that erupted upon the Russian invasion of Ukraine. The 2022 invasion was accompanied by a simultaneous struggle over digital control, both within Ukraine and Russia. On February 28, 2022, with 200,000 Russian troops within his country, Ukrainian Minister of Digital Transformation Mykhailo Fedorov sent an urgent plea to ICANN, the California-based body that manages the global Internet domain name system. Citing Russian disinformation, hate speech, the promotion of violence online, and cyber-attacks, he asked ICANN to revoke the domains ".ru.," ".рф," and ".su"—the Russian and (former) Soviet top level domains. Fedorov simultaneously wrote to RIPE Network Coordination Centre (RIPE NCC), a regional Internet registry based in Amsterdam, asking it to cancel all Internet addresses allocated to Russians. He hoped to wipe Russia off the Internet.

ICANN responded that it "does not control internet access or content," and that, in any case, its goal was "to ensure that the Internet works, not . . . to stop it from working." RIPE NCC, too, while condemning the "violent actions" against Ukraine, rejected the request, arguing that the Internet address registry should not be "used to achieve political ends." Strikingly, it cited Dutch law. If the Internet authorities had indeed removed Russian domain names or Internet addresses, faith in those authorities might have been eroded, as countries would begin wondering if they would be the next target of such actions. It would make those authorities clearly geopolitical actors.

Instead of global and regional Internet authorities, the struggle over the Russian Internet would shift to the Internet companies that provide so much of the infrastructure of the modern economy. Private U.S. enterprises were willing to take more active steps. YouTube suspended Russian state-supported media channels, while Google suspended most of its commercial services in Russia, including advertising. But Google continued to provide Russians with free services such as search, Gmail, and YouTube, and to support the Android operating system. Twitter expanded its labeling of Russian state-owned media to include tweets by third parties referencing such media. It followed EU sanctions banning such media within the EU. Like some other newspapers, the *Washington Post* lifted its paywall for users in Russia and Ukraine, hoping to make its high-quality information about the conflict more readily available.

Meta established a special operations center including Russian and Ukrainian speakers to respond more quickly to issues. It expanded third-party fact-checking capacity in Russian and Ukrainian languages and offered financial support to Ukrainian fact-checking partners. Meta labeled Russian state-controlled media outlets, stopped algorithmically recommending them, and, in accordance with EU sanctions, stopped distributing them within the European Union. In March 2022, Meta made a controversial change to its hate speech policy, temporarily allowing violent speech such as "death to the Russian invaders." While Meta's goal was to avoid removing posts by "ordinary Ukrainians expressing their resistance and fury at the invading military forces," it left the company open to the charge that it permitted calls for violence against Russian soldiers when it would not allow such calls against others. As mentioned above, later in March 2022, the Russian Internet regulator, Roskomnadzor blocked access to Facebook and Instagram.

The Telegram app, which claims a quarter of Russia's population as users, took a more equivocal path, permitting both Russian propaganda and criticism. Founded by a Russian, Pavel Durov, and his brother, Telegram is now operated by Durov from Dubai. In 2018, Russia had sought to ban Telegram for allegedly refusing to hand over encryption keys, but then lifted the ban after the company, according to the Russian government, agreed to help it combat terrorism and extremist content. In 2021, the founder of a rival messaging app warned Telegram users that Telegram could read in plain text all of the messages they had ever sent. Telegram is not end-to-end encrypted by default, unlike alternatives like WhatsApp and Signal.

These major developments following the Russian invasion of Ukraine thus reveal some key elements of digital sovereignty. First, controlling the local Internet carries global implications. Both Russia and Ukraine sought to influence global actors, both public and private, to achieve their political goals. Ukraine's efforts to banish Russia from the global Internet threatened core functions, and would, if successful, have raised alarms across the world at the control wielded by obscure, unelected institutions.

Second, Internet enterprises hold incredible power, and any government that hopes to regulate its territory must be able to regulate those enterprises. The power of Internet companies includes the ability to promote or censor information. No denial of service cyberattack against digital infrastructure is necessary when the corporation itself denies service.

Third, when governments can coopt the power of Internet companies, they gain an awesome power that can be abused. For example, Internet

enterprises can be ordered to promote the official version of the truth and censor all else. Having ejected Facebook, the Russian government could turn to the homegrown alternative it controlled—Vkontakte, which operates the country's most popular social media network and email service. In 2021, state-owned enterprise Gazprom had gained control over VKontakte, and a new CEO, Vladimir Kiriyenko, was installed. After the Russian invasion, the United States and the EU placed Kiriyenko on the sanctions list because he "supports Vladimir Putin's aim for greater control over the internet."[156]

V. The Plan for This Volume

This volume provides a comprehensive and systematic account of digital sovereignty. It grew out of the conference, "Data Sovereignty along the Digital Silk Road," organized by the editors and hosted virtually by Georgetown University and the University of Hong Kong in January 2021.

Consisting of four parts, the volume adds new theoretical perspectives on digital sovereignty and explores the cutting-edge issues it raises. Drawing mainly on various theories concerning political economy, international law, human rights, and data protection, the first part reconsiders the nature and scope of digital sovereignty. Frank Pasquale first puts forward an important idea "functional sovereignty" that highlights how large technology companies exert their authority to govern the Internet and use of digital data often in parallel to the territorial sovereign power that a government wields. To understand and tackle the nature and scope of this "functional sovereignty" is of paramount importance given that it has created a new digital political economy and affected the functioning of our liberal democracy. Revealing problems with the state boundary-based notions of sovereignty, Dan Svantesson attempts to reconceptualize sovereignty in the digital age as a political power to confront assaults on "state dignity." This theoretical approach would divert us from the state boundary-based thinking to examine the seriousness of societal effects (e.g., leakage of personal data) caused by assaults such as cyberattack. The own chapter follows, arguing that digital sovereignty has a double-edged nature. While governments must exercise it to promote citizens' freedom and welfare, governments can also abuse this

[156] Morgan Meaker, *How the Kremlin Infiltrated Russia's Facebook*, WIRED, June 1, 2022 7:00 AM, https://www.wired.com/story/vk-russia-democracy/.

power, causing harms to citizens and our democratic institutions. We call for checks and balances to regulate a government's assertion of its digital sovereignty. Anne Cheung closes this section by presenting self-sovereignty as a new theoretical basis to enhance protection of personal data. Responding to the problems exposed by the COVID-19 pandemic, she demonstrates that this approach can empower individuals to better protect their data in multiple ways.

The second part of the volume discusses major challenges at the intersection of digital sovereignty and new technological developments in sectors such as AI, e-commerce, and the sharing economy. Andrew Woods takes the lead to explore how the digital sovereignty policies and attitudes adopted in China, European Union, and the United States would impact their respective development of the AI technology. He also considers some major factors such as access to training data for us to better understand the relationship between digital sovereignty and AI. Lizhi Liu and Barry Weingast examines unique roles that China's e-commerce sector has played in improving the building blocks of its legal market infrastructure. They demonstrate that Taobao's internal operations for contract enforcement and dispute resolution have promoted China's institutional structure of economic governance. Given the growing importance of the sharing economy, Shin-yi Peng considers how regional trade agreements could deal with divergent domestic approaches to regulating sharing platforms such as Uber and Airbnb. She concludes that current regulatory practices and regulatory cooperation championed by those agreements cannot do much to harmonize the divergent regulatory approaches and encourages trade negotiators to seek new avenues of international cooperation. With a dynamic account of data and data governance in the digital finance sector, Giuliano Castellano, Ēriks Selga, and Douglas Arner identify three different financial data governance strategies that the United States, the European Union, and China have adopted based on their own policies toward market institutions and the protection of individual and public interests in data. They also discuss how the global financial market should cope with challenges posed by regulatory fragmentation and localization requirements for financial data.

As trade regulation is increasingly intertwined with digital sovereignty, the third part of the volume explores various issues and developments in the national, regional, and international regulation of data flow. Based on a study of various domestic rules governing cross-border flows of data, Henry Gao puts forward three models of constructing data sovereignty in this regard,

namely the United States' firm sovereignty model, China's state sovereignty model, and the EU's individual sovereignty model. He also considers how the different trade protection policies adopted by these countries have shaped their own regime of data governance. With a closer look at the underlying ideas, policy goals, and regulatory complexities of India's data governance, Neha Mishra reveals why India has built this nationalist regime that mainly supports its domestic digital economy. This reality, as she further shows, has largely prevented India from negotiating trade rules dealing with cross-border data flows. Mira Burri examines the extent to which preferential trade agreements, mainly concluded by the European Union and the United States with their respective trade partners, have developed regional rules governing cross-border flows of data and set up temples for further rule-making. As data governance becomes the focal part of trade negotiations, she calls for increased regulatory cooperation and legal innovation in making such rules regionally and internationally.

The fourth part of the volume presents data localization as a major form of assertion of digital sovereignty, examining its promise and pitfalls in the process of trade liberalization, data regulation, and human rights protection. Graham Greenleaf first shows that the data localization mandate normally entails six distinct forms of legal regulation, ranging from storing and processing data locally to the prohibition of exporting data. He then studies data privacy laws in the major countries along the modern "Silk Roads", finding that China, Russia, and three South Asian countries adopted all six forms of data localization and five Central Asian countries only regulate data exports. Kyung Sin Park explores the tension between data localization requirements and human rights protection norms. Internet shutdowns, as he demonstrates, can produce data localization effects that may harm the protection of human rights such as free speech and privacy. Theodore Christakis examines the rise of data localization requirements in the EU and identifies the factors contributing to this rise. He then shows how the Court of Justice of the European Union's 2020 *Schrems II* ruling has rendered such requirements more stringent.

Taken together, the brilliant contributions to this volume demonstrate both the urgency and complexity of digital sovereignty.