



2021

## Sovereignty 2.0

Anupam Chander

*Georgetown University Law Center, ac1931@georgetown.edu*


Haochen Sun

*University of Hong Kong Faculty of Law*

This paper can be downloaded free of charge from:  
<https://scholarship.law.georgetown.edu/facpub/2404>  
<https://ssrn.com/abstract=3904949>

---

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.  
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Computer Law Commons](#), [Intellectual Property Law Commons](#), and the [International Law Commons](#)

# Sovereignty 2.0

Anupam Chander<sup>\*</sup> and Haochen Sun<sup>\*\*</sup>

Digital sovereignty—the exercise of control over the internet—is the ambition of the world’s leaders, from Australia to Zimbabwe, a bulwark against both foreign state and foreign corporation. Governments have resoundingly answered first-generation internet law questions of who if anyone should regulate the internet—they all will. We now confront second generation questions—not *whether*, but *how* to regulate the internet. We argue that digital sovereignty is simultaneously a necessary incident of democratic governance and democracy’s dreaded antagonist. As international law scholar Louis Henkin taught us, sovereignty can insulate a government’s worst ills from foreign intrusion. Assertions of digital sovereignty, in particular, are often double-edged—useful both to protect citizens and to control them. Digital sovereignty can magnify the government’s powers by making legible behaviors that were previously invisible to the state. Thus, the same rule can be used to safeguard or repress—a feature that legislators across the Global North and South should anticipate by careful checks and balances.

---

<sup>\*</sup> Professor of Law, Georgetown University. J.D. Yale; A.B. Harvard. This paper grew out of the conference, Data Sovereignty along the Digital Silk Road, organized by the authors and hosted virtually by Georgetown University and the University of Hong Kong in January 2021. The authors thank Kelly Chen, Kealey Clemens, Elizabeth Goodwin, Noelle Wurst, Ming Yi, and librarian Heather Casey for excellent research assistance.

<sup>\*\*</sup> Associate Professor of Law, University of Hong Kong Faculty of Law. LL.M., Harvard Law School; S.J.D., Duke Law School.

Introduction.....	3
I. From Hobbes to Zuckerberg: The Rise of Digital Sovereignty .....	8
A. Defining “Digital Sovereignty” .....	9
B. China: Inventing Digital Sovereignty .....	11
C. The EU: Embracing Digital Sovereignty .....	15
D. Russia: Promoting the Runet .....	16
E. The United States: Digital Sovereignty by Default.....	18
F. The Global South: Avoiding Data Colonialism .....	19
II. How Digital Sovereignty Is Different .....	21
A. Always global .....	21
B. Against corporations.....	22
C. More control .....	23
D. Enables protectionism .....	24
III. The Double-Edged Sword of Digital Sovereignty .....	26
A. Speech.....	27
B. Privacy .....	29
C. National Security .....	31
Conclusion .....	36

## Introduction

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.<sup>1</sup> Sovereignty would prove impossible over a world of bits, with the internet simply routing around futile controls.<sup>2</sup> But reports of the death of sovereignty over the internet proved premature. Consider just the last few months:

- On the eve of what was to be the world’s biggest initial public offering ever in November 2020, 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.”<sup>3</sup> Chastened after Beijing’s intervention, Ant announced that it would “embrace regulation,” and Chinese netizens declared Jack Ma duly “tamed.”<sup>4</sup>
- In June 2021, France fined Google \$593 million dollars for failing to follow an order to negotiate with news publishers to compensate them for displaying snippets of news items before linking.<sup>5</sup> In July 2021, Luxembourg’s privacy regulator fined Amazon \$887 million for data protection violations.<sup>6</sup> 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.<sup>7</sup> Even Facebook

---

<sup>1</sup> See John P. Barlow, *The Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION (July 16, 2021, 1:59 PM), <https://www.eff.org/cyberspace-independence>.

<sup>2</sup> As John Gilmore famously announced, “The Net interprets censorship as damage and routes around it.” See Philip Elmer-DeWitt & David S. Jackson, *First Nation in Cyberspace*, TIME MAGAZINE, Dec. 3, 1993, at 62.

<sup>3</sup> See 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>.

<sup>4</sup> *Id.*

<sup>5</sup> 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>.

<sup>6</sup> 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/>. The previous highest fine issued by the Luxembourg data protection authority was 18,000 euros. *GDPR Enforcement Tracker*, <https://www.enforcementtracker.com/> (last visited, August 2, 2021, at 7:35 pm).

<sup>7</sup> See Sam Schechner & Parmy Olson, *Google Faces EU Antitrust Probe of Alleged Ad-Tech Abuses*, WALL STREET JOURNAL (June 22, 2021), <https://www.wsj.com/articles/google-faces-eu-antitrust-probe-of-alleged-ad-tech-abuses-11624355128>; Natasha Lomas, *Europe Charges Apple with Antitrust Breach, Citing Spotify App Store Complaint*, TECH CRUNCH (Apr. 30, 2021), <https://techcrunch.com/2021/04/30/europe-charges-apple-with-antitrust-breach-citing-spotify-app-store-complaint/>; Adam Satariano, *Facebook Faces Two Antitrust Inquiries in Europe*, NY TIMES

Dating receives unwanted attention from the British competition authority.<sup>8</sup>

- 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 Federal Trade Commission (FTC) seeks to compel Facebook to divest WhatsApp and Instagram, while investigating Amazon for competing with merchants that use its platform.<sup>9</sup> The federal government and all but two U.S. states and are bringing antitrust claims against Google,<sup>10</sup> and the U.S. Justice Department is investigating Apple's App Store.<sup>11</sup>
- Assertions of digital sovereignty are hardly limited to Western nations. After Twitter deleted tweets of its President that warned 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 had gone even further, ordering a complete shutdown of the internet, with President Yoweri Museveni explaining that Facebook had deleted pro-government accounts as manipulative.<sup>12</sup> Uganda followed the example of Zimbabwe,

---

(June 4, 2021) <https://www.nytimes.com/2021/06/04/business/facebook-eu-uk-antitrust.html>; Alina Selyukh, *Amazon Faces Antitrust Charges From European Regulators*, NPR (Nov. 10, 2020), <https://www.npr.org/2020/11/10/879643610/amazon-faces-antitrust-charges-from-european-regulators>.

<sup>8</sup> See U.K. Competition and Markets Authority, *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>.

<sup>9</sup> Federal Trade Commission, 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> (tech in general and the FTC); *Factbox: How Big Tech Is Faring Against U.S. Lawsuits and Probes*, REUTERS (July 13, 2021), <https://www.reuters.com/technology/big-tech-wins-two-battles-fight-with-us-antitrust-enforcers-2021-06-29/>; See Brent Kendall, *Amazon Seeks Recusal of FTC Chairwoman Lina Khan in Antitrust Investigations of Company*, WALL STREET JOURNAL (June 30, 2021), <https://www.wsj.com/articles/amazon-seeks-recusal-of-ftc-chairwoman-lina-khan-in-antitrust-investigations-of-company-11625067962> (Amazon).

<sup>10</sup> See Department 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> (Google); Rachel Lerman & Marcy Gordon, *States Led by Texas Target Google in New Antitrust Probe*, ASSOCIATED PRESS (Sept. 9, 2019), <https://apnews.com/article/texas-district-of-columbia-ne-state-wire-ap-top-news-social-platforms-b9d35b1e07b14f3b923c35e7778295ee> (fifty U.S. states and territories suing Google); Matt O'Brien, *Big Tech Faces a New Set of Foes: Nearly All 50 US States*, ASSOCIATED PRESS (Sept. 10, 2019), <https://apnews.com/article/business-district-of-columbia-us-news-ap-top-news-ut-state-wire-8fae76b9b37d473caff2c94a59029a57>.

<sup>11</sup> See Leah Nylen, *Apple's Easy Ride 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> (Apple); *Factbox: How Big Tech Is Faring Against U.S. Lawsuits and Probes*, REUTERS (July 13, 2021), <https://www.reuters.com/technology/big-tech-wins-two-battles-fight-with-us-antitrust-enforcers-2021-06-29/>.

<sup>12</sup> 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/>.

which had responded to anti-government protests in 2019 by shuttering the internet.<sup>13</sup> The state (both nation-state as well as nearly every U.S. state) strikes back.<sup>14</sup>

Scholars are sharply divided about the increasing assertion of what is called variously “data sovereignty” or “digital sovereignty.”<sup>15</sup> Some scholars see it as a natural extension of traditional Westphalian sovereignty to the twenty-first century.<sup>16</sup> 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.<sup>17</sup> Other scholars, however, worry that data sovereignty will break the web apart, jeopardizing its numerous global benefits.<sup>18</sup> 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.”<sup>19</sup>

We recognize the importance of digital sovereignty to protect privacy, ensure consumer protection, promote competition, and enable law enforcement. Developing countries should indeed seek to ensure that the digital economy does not leave them behind. However, even as scholars understandably seek to protect individual rights through digital sovereignty, they often neglect the critique that sovereignty can insulate human rights abuses from outside scrutiny. Away with the “S-word,” the preeminent human rights theorist Louis Henkin cautioned.<sup>20</sup> We argue that Henkin’s concern is even graver with respect digital sovereignty, which presents greater risk of totalitarian control. While digital sovereignty may well be a geopolitical necessity in opposition to both foreign governments and foreign corporations, digital sovereignty also allows a government to assert enormous powers over one’s own citizens, and thus deserves

---

<sup>13</sup> 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>.

<sup>14</sup> 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 (July 13, 2021), <https://www.channele2e.com/business/compliance/big-tech-antitrust-regulatory-breakup-updates/>.

<sup>15</sup> We explore various definitions of the terms in Part I, A below.

<sup>16</sup> 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).

<sup>17</sup> See Renata Avila Pinto, *Digital Sovereignty or Digital Colonialism*, 27 SUR - INT’L J. ON HUM RTS. 15 (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).

<sup>18</sup> 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.”).

<sup>19</sup> *Id.* at 1409.

<sup>20</sup> See Louis Henkin, *That “S” Word: Sovereignty, and Globalization, and Human Rights, et Cetera*, 68 FORDHAM L. REV. 1, 11 (1999) (observing that he “use[s] the word only to stop using it”).

exacting scrutiny. We call this the double-edged sword of digital sovereignty: digital sovereignty both enables the protection of residents, and their control.

The ongoing tech wars between the U.S. and China, as our article shows, epitomize the double-edged sword of digital sovereignty. In 2020, the Trump Administration issued a series of executive orders that had the effect of banning TikTok's and WeChat's operations in the U.S. on national security grounds.<sup>21</sup> While dealing with potential threats posted by China's collection of data through these platforms, the government turned a blind eye to the serious harm its orders had caused to speech protection.<sup>22</sup> The upshot was that more than 100 million U.S. users<sup>23</sup> would have been muted on TikTok, a digital platform crucial for social activities during the COVID-19 pandemic and for politics on the eve of an election.<sup>24</sup> American courts reacted to the dark side of the U.S. government's assertions of digital sovereignty. It enjoined those sweeping orders against TikTok and WeChat, because they "burden[ed] substantially more speech than is necessary to serve the government's significant interest in national security."<sup>25</sup>

Our article is the first comprehensive account of digital or data sovereignty.<sup>26</sup> We survey the various ways in which states are asserting digital sovereignty. We argue that digital

---

<sup>21</sup> See Anupam Chander, *Protecting the Global Internet from Technology Cold Wars*, COMMUNICATIONS OF THE ACM (forthcoming 2021).

<sup>22</sup> See Eva Galperin et al., *TikTok Ban: A Seed of Genuine Security Concern Wrapped in a Thick Layer of Censorship*, ELECTRONIC FRONTIER FOUNDATION (Aug. 4, 2020), <https://www.eff.org/zh-hant/deeplinks/2020/08/tiktok-ban-seed-genuine-security-concern-wrapped-thick-layer-censorship> ("Banning Americans from using the TikTok app would infringe the First Amendment rights of those users to express themselves online."); Gregg Leslie, *TikTok and the First Amendment*, SLATE (Sept. 29, 2020), <https://slate.com/technology/2020/09/tiktok-wechat-first-amendment-free-speech.html> (arguing that "the First Amendment should save TikTok [and WeChat]"); Shelly Banjo & Misyrlena Egkolfopoulou, *TikTok Teens Try To Trick Trump Campaign, Again*, BLOOMBERG (July 10, 2020), <https://www.bloomberg.com/news/articles/2020-07-09/tiktok-teens-try-to-trick-trump-campaign-again> (reporting that users "believe Trump is trying to take TikTok away because of national security, but more to retaliate against activism on the app and all the videos about him that drag him through the mud").

<sup>23</sup> Alex Sherman, *TikTok Reveals Detailed User Numbers for the First Time*, CNBC (Aug. 24, 2020), <https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html> ("More than 100 million Americans are monthly active users today, the company said earlier this month. The company also revealed it has more than 50 million daily U.S. users.").

<sup>24</sup> See Taylor Lorenz, *This Is Why You Heard About TikTok So Much in 2020*, NY TIMES (Feb. 26, 2021), <https://www.nytimes.com/2020/12/31/style/tiktok-trends-2020.html> (discussing how TikTok transformed business, entertainment, news, activism and social connection in 2020); Jana Feldkamp, *The Rise of TikTok: The Evolution of a Social Media Platform During COVID-19*, in DIGITAL RESPONSES TO COVID-19 73-85 (Hovestadt C., Recker J., Richter J., Werder K. eds., 2021).

<sup>25</sup> *U.S. WeChat Users Alliance, et al., v. Donald J. Trump, et al.*, No. 3:20-cv-05910-LB, at 18 (N.D. Cal. Sep. 19, 2020). See also, *TikTok Inc., et al., v. Donald J. Trump, President of the United States, et al.*, No. 1:20-cv-02658-CJN (Opinion) (D.D.C. Sep. 27, 2020).

<sup>26</sup> Cf. Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328 (2018) (arguing that national attempts to regulate the global cloud are legitimate, and can be reasonably disciplined through judicial

sovereignty is not merely a twenty-first century extension of traditional sovereignty, necessary to discipline the corporations that have enormous power in our lives, but that also that digital sovereignty is especially susceptible to hijacking by abusive governments.

Our argument helps explain a puzzling feature of discussions of digital sovereignty: observers generally welcome digital sovereignty efforts by governments in the Global North, but deplore such efforts by governments in the Global South.<sup>27</sup> In the former case, digital sovereignty is recognized as the government protecting citizens—either from foreign governments or corporations. In the latter case, digital sovereignty is seen as the government hijacking the internet to protect itself. This is true across a range of issues, from content moderation, to data privacy, to data localization, to national security. The double-edged nature of digital sovereignty also means that we sometimes see only the negative end of digital regulations. The American government, academic, and media have rightly observed how the Chinese government’s assertions of digital sovereignty beefed up its political control and trampled on human rights through measures such as Internet filtering, digital surveillance, and data misuse. This sometimes means that we fail to recognize aspects of these laws that protect citizen’s rights. Notably, China has been actively protecting citizens’ data privacy rights through waves of legislative proposals, regulatory measures, and judicial decisions (though we point out dangers in this exercise below<sup>28</sup>).

Our argument exposes a difficulty in one popular framing of digital sovereignty as an effort to thwart Chinese technology dominance on the grounds that Chinese technology inherently promotes greater authoritarian controls. We agree that technologies are never

---

doctrines of sovereign deference); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018) (; Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 *Philosophy & Technology* 369, 375 (2020) (arguing that “the best answer to the multinationals’ control of the digital is probably the establishment of a (de jure and not only a possibly de facto) supranational digital sovereignty, at the EU level”); Theodore Christakis, “*European Digital Sovereignty*”: *Successfully Navigating Between the “Brussels Effect” and Europe’s Quest for Strategic Autonomy*, *Studies on Internet Governance*, <https://cesice.univ-grenoble-alpes.fr/actualites/2020-12-15/european-digital-sovereignty-successfully-navigating-between-brussels-effect-and-europe-s-quest>.

<sup>27</sup> For example, when India ordered MasterCard to stop issuing new cards in the country because of a failure to comply with requirements to store the data in India, reports in the media criticized the curb as “egregious.” See Andy Mukherjee, *Sorry, No Mastercard? Digital Trade Needs Rules*, BLOOMBERG OPINION (July 15, 2021), <https://www.bloomberg.com/opinion/articles/2021-07-15/india-s-data-clampdown-on-mastercard-shows-need-for-biden-digital-trade-deal>. Similar concerns about the transfer of data abroad, when raised in Europe, have often been seen as privacy protective (whether justified or not). Hong Kong recently real-name SIM card registration introduced to much alarm. But real-name SIM card registration is already a feature in some 155 countries, including Australia, France, and Germany. See *A List of Mandatory ‘real name’ prepaid SIM card registration Country?*, BUZZSIM, <https://buzzsim.com/mandatory-real-name-registration-for-prepaid-sim-card-in-different-countries/>; *Timeline of SIM Card Registration Laws*, PRIVACY INTERNATIONAL (Apr. 21, 2021), <https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws>.

<sup>28</sup> See *infra* notes 183-190 and accompanying text.



neutral<sup>29</sup>—that they can be more or less adaptable for authoritarian purposes. However, this framing of an ethical North vs. and unethical South obscures the fact that regulatory systems everywhere have to be better prepared for the abuses of technology by governments keen on maintaining their power. The recent revelations of the widespread use by countries in Europe and across the world of Western surveillance provider NSO spyware dramatize this concern.<sup>30</sup> There is no need for a government to adopt Chinese technologies,<sup>31</sup> if you can buy your spyware off the shelf from Western suppliers.

We argue here for digital sovereignty, but within a system of checks and balances, and limited to protect the virtues of the global internet. Digital sovereignty is both necessary and dangerous. It is both merely an incident to popular sovereignty, and its *bête noire*.

This article proceeds as follows. Part I describes the emergence of Sovereignty, 2.0. Part II observes the unique characteristics of this new twenty-first century sovereignty. Part III explores the double-edged sword of digital sovereignty through recent regulatory interventions.

## I. From Hobbes to Zuckerberg: The Rise of Digital Sovereignty

When Thomas Hobbes imagined an “Artificiall Man” in the form of a state,<sup>32</sup> he was not picturing Facebook. But the reality is that modern leviathans like Facebook and Google, and even Reddit and Twitter, exercise enormous power over our lives. 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.

After defining digital sovereignty, we review below the effort to attain data sovereignty in a few key jurisdictions. Our review reveals at least three different motivations for assertions of data 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.

---

<sup>29</sup> See Anupam Chander & Vivek Krishnamurthy, *The Myth of Platform Neutrality*, 2 GEO. L. TECH. REV. 400 (2018).

<sup>30</sup> See *infra* notes 205-219 and accompanying text.

<sup>31</sup> See Paul Mozur et al., *Made in China, Exported to the World: The Surveillance State*, NY TIMES (Apr. 24, 2019), <https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html>.

<sup>32</sup> THOMAS HOBBS, LEVIATHAN (1651), <https://www.gutenberg.org/files/3207/3207-h/3207-h.htm> (“[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 Sovereigne Power; and at the other end to their own Ears.”).

## A. 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 territory.<sup>33</sup> 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.”<sup>34</sup> The tension between the notion of “digital sovereignty” and the territorial foundation for sovereignty disappears when we recognize 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.”<sup>35</sup> Dan Svantesson rightly observes that sovereignty should not have to be all-or-nothing, and so perhaps Woods’ requirement of exclusivity is unnecessarily strict for a claim of data sovereignty.<sup>36</sup> 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”).<sup>37</sup> It seems clear that multiple states are able to order the same firm how to operate, with occasional conflicts in approaches.<sup>38</sup>

Ke Xu divides sovereignty in cyberspace into three layers: physical layer (sovereignty over physical internet infrastructure and activities), the code layer (sovereignty over domain names, internet standards, and regulations), and the data layer.<sup>39</sup>

Like Hobbes, Luciano Floridi begins by theorizing individual sovereignty, which he defines in twenty-first century terms as “self-ownership, especially over one’s own body, choices, and data,”<sup>40</sup> and then extends this to “digital sovereignty,” which he defines as the “control of

---

<sup>33</sup> 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.”

<sup>34</sup> Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 360 (2018).

<sup>35</sup> *Id.* at 360-361.

<sup>36</sup> Dan Svantesson, A Starting Point for Re-thinking ‘Sovereignty’ for the Online Environment (draft on file with author).

<sup>37</sup> Woods, *supra* note 34, at 364.

<sup>38</sup> 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 U.S. would be illegal under Irish law.

<sup>39</sup> Ke Xu, *Data Security Law: Location, Position and Institution Construction*, 3 BUS. & ECON. L. REV. 57 (2019).

<sup>40</sup> Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHILOSOPHY AND TECHNOLOGY 369, 371 (2020).

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).<sup>41</sup>

Data sovereignty, as argued by Paul Rosenzweig, may also be framed as a question: which sovereign controls the data?<sup>42</sup> The core issue is one of jurisdiction, which is, of course, complicated by the borderless nature of the internet.<sup>43</sup> “In short, the question is: ‘Whose law is to be applied?’<sup>44</sup> 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.’”<sup>45</sup> 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,<sup>46</sup> or simply “sovereignty in a digital age.”<sup>47</sup> 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 interchangeably with “data sovereignty” because a distinction between dominion over “data” and dominion over the “digital” is hard to maintain. 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:<sup>48</sup>

	Data Sovereignty		Digital Sovereignty	
	Academic	Other	Academic	Other
2019-2021	271	1378	44	731

<sup>41</sup> *Id.* at 370-371.

<sup>42</sup> See Paul Rosenzweig, *The International Governance Framework for Cybersecurity*, 37 CAN.-U.S. L.J. 405, 421 (2012).

<sup>43</sup> See *id.*

<sup>44</sup> *Id.* at 422.

<sup>45</sup> *Id.*

<sup>46</sup> 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, [http://www.senat.fr/fileadmin/Fichiers/Images/redaction\\_multimedia/2019/2019\\_Infographies/2019\\_1004\\_infog\\_Souverainete\\_numerique\\_021019.pdf](http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2019/2019_Infographies/2019_1004_infog_Souverainete_numerique_021019.pdf) (Oct. 2019).

<sup>47</sup> Paul Timmers, *Challenged by “Digital Sovereignty,”* 23 (6) J. INTERNET L. 1, 18 (2019).

<sup>48</sup> 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 & SOCIETY 2305, 2306 (2019). Note that the “other” category includes newspapers, trade journals, magazines, reports, blogs, books, and working papers.

## B. 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 — "a far-ranging attempt to harness emerging information technologies for policing."<sup>49</sup> Henry Gao observes that Chinese digital sovereignty evolved through different phases—physical controls, and then controls over the software layer and content.<sup>50</sup> In other words, it went up the internet stack. As James Fallows writes in a classic Western account of "the Great Firewall of China," "In China, the Internet came with choke points built in."<sup>51</sup> 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 data sovereignty.<sup>52</sup> 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.<sup>53</sup> However, sometimes the firewall causes collateral impact on internet freedom beyond China's borders through DNS pollution, which blocks access to websites by users in other countries by inadvertently impeding their traffic.<sup>54</sup>

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."<sup>55</sup> The link 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 internal affairs.<sup>56</sup> 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,

---

<sup>49</sup> Lorand Laskai, *Nailing Jello to the Wall*, in JANE GOLLEY, LINDA JAIVIN, & LUIGI TOMBA, CONTROL 192, 194 (2017).

<sup>50</sup> Henry Gao, *Data Regulation with Chinese Characteristics*, in Mira Burri (ed.), Big Data and Trade 245, 248 (2021) (noting that 1996 and 1997 Chinese "regulations all focused on the Internet hardware," while attention was paid later to software and content).

<sup>51</sup> James Fallows, *The Connection Has Been Reset*, ATLANTIC (Mar. 2008), <https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/>.

<sup>52</sup> Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 Ohio St. Tech. L.J. 395, 403 (2020); [http://www.china.org.cn/government/whitepaper/2010-06/08/content\\_20207978.htm](http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm).

<sup>53</sup> See *id.* at 408, 439.

<sup>54</sup> See *id.* at 408, 439-41.

<sup>55</sup> See *id.* at 399.

<sup>56</sup> 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").

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.”<sup>57</sup>

China has escalated the tech cold war in 2021. 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.<sup>58</sup> Even though Didi’s stock price plummeted, Chinese media celebrated the “rise of data sovereignty.”<sup>59</sup>

China’s conception of digital sovereignty is rooted, Anqi Wang writes, in traditional notions of territorial sovereignty<sup>60</sup> and officially justified by concern for national and ideological security.<sup>61</sup> China supports to a “state-centric multilateralism” model of internet governance,<sup>62</sup> which holds that states, not private sector actors like ICANN, should be driving internet governance.<sup>63</sup> In contrast, the “bottom-up multi-stakeholderism” subscribed to by the US and other Western countries<sup>64</sup> holds that the private sector and civil society should remain key players in internet governance.<sup>65</sup> Western “information freedom” approach to the internet<sup>66</sup> is perceived as a threat to “Chinese ideological security” and a tool of cultural imperialism.<sup>67</sup> 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

---

<sup>57</sup> See *id.* 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/>.

<sup>58</sup> See Jacky Wong, *Didi and the Big Chill on China’s Big Data*, WALL STREET JOURNAL (July 5, 2021), <https://www.wsj.com/articles/didi-and-the-big-chill-on-chinas-big-data-11625479452>.

<sup>59</sup> 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 US 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.”).

<sup>60</sup> See Wang, *supra* note 52, at 397.

<sup>61</sup> See *id.* at 424 (explaining China views cybersecurity as another national security domain alongside land, sea, air, and space).

<sup>62</sup> See *id.* at 443-44.

<sup>63</sup> See *id.* (explaining that China opposes the current system where a US corporation, ICANN (Internet Corporation for Assigned Names and Numbers), controls root ownership).

<sup>64</sup> See *id.* at 399.

<sup>65</sup> See *id.* at 444.

<sup>66</sup> See *id.* at 400.

<sup>67</sup> See *id.* at 406.

“develop a cohesive, socialist nation.”<sup>68</sup> 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.”<sup>69</sup>

China sees US internet infrastructure hegemony as a threat to its digital sovereignty.<sup>70</sup> In 2016, President Xi stated, “the fact that [the internet’s] core technology is controlled by others is our greatest hidden danger.”<sup>71</sup> Accordingly, the government has been investing heavily in research and development of internet technology<sup>72</sup> and “territorializing critical infrastructure”<sup>73</sup> to escape Western technical and physical network dependence. Part of this effort has been a proliferation of Critical Information Infrastructure (CII) regulations,<sup>74</sup> including data localization regulations through the 2017 Cybersecurity Law (CSL).<sup>75</sup> Not only does Article 37 of the CSL require that data and personal information originating in China be stored within China, critical information infrastructure operators must also undergo “security assessments” before that data can be transferred abroad.<sup>76</sup> (We describe later the first such security assessment—against the ride-hailing company Didi.<sup>77</sup>)

Content regulation and censorship is another integral component of China’s “information sovereignty” on the internet.<sup>78</sup> Though China’s approach to content regulation is more extreme than other countries,<sup>79</sup> it rejects accusations that cyber sovereignty policies simply mask authoritarian control.<sup>80</sup> Instead, the government claims to censor “subversive,” “harmful,”

---

<sup>68</sup> *See id.* at 407.

<sup>69</sup> *Xi Jinping gives speech at Cybersecurity and Informatization Work Conference*, CHINA COPYRIGHT AND MEDIA (Apr. 19, 2016), <https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/>.

<sup>70</sup> *See* Wang, *supra* note 52, at 404-05 (explaining that China perceives US corporate and civil society control over domain names and US-made infrastructure as favoring US interests).

<sup>71</sup> *See id.* at 405.

<sup>72</sup> *See id.* at 434, 436.

<sup>73</sup> *See id.* at 434.

<sup>74</sup> *See id.* at 436-37.

<sup>75</sup> *See id.* at 408, 456.

<sup>76</sup> *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); Reed Smith, *Cross-Border Data Transfers: CSL vs. GDPR* (January 2, 2018), <https://www.reedsmith.com/en/perspectives/2018/01/cross-border-data-transfer-csl-vs-gdpr>; 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>.

<sup>77</sup> *See infra* notes 183-189 and accompanying text.

<sup>78</sup> *See* Wang, *supra* note 52, at 452.

<sup>79</sup> *See id.* at 466.

<sup>80</sup> *See id.* at 416.

“obscene,” or “malicious” content while welcoming “kind criticism.”<sup>81</sup> 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.”<sup>82</sup> The Theoretical Studies Center Group of CAC also commented in 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.”<sup>83</sup>

Some of the measures China takes to regulate content and maintain a “clear cyberspace”<sup>84</sup> include blocking VPN access, algorithms that divert searches, the Real Name Registration Policy,<sup>85</sup> 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.<sup>86</sup> However, standards for what information is “erroneous” or in violation of the law remain unclear.<sup>87</sup> 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.<sup>88</sup> 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.<sup>89</sup>

Through its “Digital Silk Road,” which adopts one of the authors’ framing of the internet as the “Electronic Silk Road,”<sup>90</sup> 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 AI.<sup>91</sup> By increasing developing African and Eurasian nations’ internet access,<sup>92</sup> as well as their dependence on Chinese technology, China acquires

---

<sup>81</sup> 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, 422.

<sup>82</sup> Elsa Kania et al., *China’s Strategic Thinking on Building Power in Cyberspace*, NEW AMERICA (Sept. 25, 2017), <https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace>; Wang, *supra* note 52, at 453; see also Gravett, *supra* note 76, at 131.

<sup>83</sup> See Wang, *supra* note 52, at 456.

<sup>84</sup> See *id.* at 455.

<sup>85</sup> See *id.* at 456; Gravett, *supra* note 76, at 130 (describing a 2017 law that makes social media companies register users with their real names).

<sup>86</sup> See Wang, *supra* note 52, at 458.

<sup>87</sup> See *id.*

<sup>88</sup> See *id.* at 461, 464.

<sup>89</sup> See *id.*

<sup>90</sup> ANUPAM CHANDER, *THE ELECTRONIC SILK ROAD* (2013).

<sup>91</sup> See *id.* at 441.

<sup>92</sup> See *id.* at 417.

soft power, while creating new markets for Chinese technology exports and e-commerce.<sup>93</sup> 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.<sup>94</sup> Thus, even as the Chinese government worries about foreign influences via the internet, many other governments worry about the Chinese government. China looms especially large in the geopolitics that are driving many assertions of digital sovereignty.

### C. The EU: Embracing Digital Sovereignty

Nowhere have calls for digital sovereignty been more intense than 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.”<sup>95</sup> 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.”<sup>96</sup> 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.<sup>97</sup> 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.”<sup>98</sup>

---

<sup>93</sup> See *id.* at 447; Gravett, *supra* note 76, at 131 (international consensus building).

<sup>94</sup> See Wang, *supra* note 52, at 441.

<sup>95</sup> Chander, *supra* note 90, at 40.

<sup>96</sup> 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 (Jul. 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, January 18, 2010).

<sup>97</sup> 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).

<sup>98</sup> 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](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, 690-1 (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



EU digital sovereignty has been expressed perhaps most fully through a robust assertion of data protection law. The EU's data protection law covers companies based in the EU, but also foreign companies that target the EU residents and process information about them. This has made the EU into an internet regulatory superpower.<sup>99</sup>

The German government announced in July 2020 that it would “establish digital sovereignty as a leitmotiv of European digital policy.”<sup>100</sup> The European Commission similarly declared its intention to “strengthen its digital sovereignty and set standards, rather than following those of others.”<sup>101</sup>

#### D. 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 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.<sup>102</sup> 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.”<sup>103</sup> In 2019, Vladimir Putin signed the “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 cases.<sup>104</sup> Ironically, given Russian prolific interventions in elections abroad, Russian demands for a sovereign internet are driven in part by claims of

---

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>.

<sup>99</sup> ANU BRADFORD, THE BRUSSELS EFFECT (noting that “the EU remains an influential superpower that shapes the world in its image”); Anupam Chander, Margot Kaminski, & William McGeeveran, *Catalyzing Privacy*, MINN. L. REV. (2020)

<sup>100</sup> *Together for Europe's recovery: Programme for Germany's Presidency of the Council of the EU 2020*, at 8 (2020), <https://www.eu2020.de/blob/2360248/978a43ce17c65efa8f506c2a484c8f2c/pdf-programm-en-data.pdf>

<sup>101</sup> 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>.

<sup>102</sup> 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).

<sup>103</sup> See Jane Wakefield, *Russia 'Successfully Tests' Its Unplugged Internet*, BBC NEWS (Dec. 24, 2019), <https://www.bbc.com/news/technology-50902496> (quoting Professor Alan Woodward as saying that the Runet would keep Russian citizens “within their own bubble”).

<sup>104</sup> See Ksenia Koroleva et al., *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/>.

“information warfare” waged by Western countries against the Russian government.<sup>105</sup> One of the goals of the Runet is to protect the Russian internet from “external negative influences.”<sup>106</sup>

Russia employs a common and highly controversial tactic for implementing digital sovereignty: data localization.<sup>107</sup> 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.<sup>108</sup> 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.<sup>109</sup> 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.<sup>110</sup> Roskomnadzor has also threatened to throttle Google’s traffic if it refuses to localize data.<sup>111</sup>

---

<sup>105</sup> Orlova, *supra* note 102, at 231.

<sup>106</sup> 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>.

<sup>107</sup> For an argument that data localization both undermines domestic development and increases the power of local authoritarians, see Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

<sup>108</sup> 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 (Rus.).

<sup>109</sup> See Adrian Shahbaz et al., *Special Report 2020: User Privacy or Cyber Sovereignty?*, FREEDOM HOUSE, <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>; *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>.

<sup>110</sup> 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/>.

<sup>111</sup> 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>.

## E. The United States: Digital Sovereignty by Default

One nation is more likely to criticize data sovereignty than to embrace it: the United States.<sup>112</sup> 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 U.S. exercised data sovereignty from the start. The Federal Trade Commission, for example, cited GeoCities for privacy failures as early as 1998.<sup>113</sup>

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.<sup>114</sup> 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 U.S. should not impose its interpretation of copyright law on foreign nations.<sup>115</sup>

In part because top level domain names are indexed on a domain name server in Virginia, the United States government has routinely seized domain names of sites that violate domestic law. Karen Kopel, writing in a student note in 2013, observes: "Since its inception over two and a half years ago, [U.S. 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."<sup>116</sup> But these

---

<sup>112</sup> See Couture & Toupin, *supra* note 48, at 2313 ("Within the United States, digital sovereignty (or related terms) usually have negative connotations across the political spectrum."). For example, the US 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/>.

<sup>113</sup> *FTC, GeoCities Settle on Privacy*, CNET (Aug. 13, 1998), <https://www.cnet.com/tech/services-and-software/ftc-geocities-settle-on-privacy/>; GeoCities, Docket No. C-3850 F.T.C. (1999), [https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do .htm](https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do.htm).

<sup>114</sup> See *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/>.

<sup>115</sup> N.Y. Times (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."). See Matt Richtel, *Russian Company Cleared of Illegal Software Sales*, NY TIMES (Dec. 18, 2002), <https://www.nytimes.com/2002/12/18/business/technology-russian-company-cleared-of-illegal-software-sales.html>.

<sup>116</sup> 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).

enforcement actions, Kopel suggests, lack sufficient process and may infringe on First Amendment concerns.<sup>117</sup>

The fact that the largest internet companies are based in the United States also means that data about Americans is typically stored in the United States. This allows prosecutors to use traditional judicial processes within 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.<sup>118</sup> Congress intervened to amend the law to grant authority to prosecutors to use judicial process to require companies to produce data held abroad.<sup>119</sup>

But earlier enforcement efforts against internet enterprises do not seem to compare with the regulatory demands that resound across the political spectrum in the United States. If there ever was a laissez-faire era for U.S. internet regulation,<sup>120</sup> that era is distinctly over.<sup>121</sup>

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."<sup>122</sup>

#### F. The Global South: Avoiding Data Colonialism

Even as access to the internet has grown dramatically,<sup>123</sup> 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 materials (now in the form of data) and markets for Western manufacture (in the form of processed information).

---

<sup>117</sup> *Id.* at 885-893.

<sup>118</sup> *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016).

<sup>119</sup> USA CLOUD Act, 18 U.S.C. § 2713 et seq.

<sup>120</sup> For a comparative history of U.S. internet regulation, see Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639 (2014).

<sup>121</sup> 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>. See *supra* notes 7-14 and accompanying text (describing antitrust claims against big technology companies).

<sup>122</sup> U.S. TRADE REPRESENTATIVE, 2021 NATIONAL TRADE ESTIMATE REPORT ON FOREIGN TRADE BARRIERS 216 (2021).

<sup>123</sup> About half of the world's people now have internet access. World Bank, *Individuals using the Internet* (undated), <https://data.worldbank.org/indicator/IT.NET.USER.ZS>.

In 2021, South Africa published a draft National Data and Cloud Policy that explicitly seeks to “promote South Africa’s data sovereignty.”<sup>124</sup> 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.”<sup>125</sup> 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.” The draft policy also announces, “Data 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.<sup>126</sup> 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.”<sup>127</sup> 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.<sup>128</sup>

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.<sup>129</sup> In the battle between developing state 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

---

<sup>124</sup> South Africa Dept. of Comm. & Digital Tech., Invitation to Submit Written Comments on the Proposed National Data and Cloud Policy 11, Apr. 1, 2021.

<sup>125</sup> See *Data Generated in SA Is the Property of SA, Says New Draft Govt Policy – And Cops Need Access*, BUSINESS 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>.

<sup>126</sup> African Union, The Digital Transformation Strategy For Africa (2020-2030), <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>.

<sup>127</sup> *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 (Jul. 6, 2020), <https://www.crossborderdataforum.org/how-african-countries-can-benefit-from-the-emerging-reform-initiatives-of-cross-border-access-to-electronic-evidence/>.

<sup>128</sup> Dan Swinhoe, *Senegal to Migrate All Government Data and Applications to New Government Data Center*, DATA CENTER DYNAMICS (June 23, 2021), <https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/>.

<sup>129</sup> *Nigerian Govt Accuses Twitter of Double Standards, Supporting Secessionists*, BUSINESS STANDARD (June 3, 2021), [https://www.business-standard.com/article/international/nigerian-govt-accuses-twitter-of-double-standards-supporting-secessionists-121060300481\\_1.html](https://www.business-standard.com/article/international/nigerian-govt-accuses-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.*

internet. This may be because government political censorship may be less likely to be complied with by the foreign platforms.

Indigenous peoples are also seeking data 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.”<sup>130</sup> 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 have relationships with.”<sup>131</sup>

## II. 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 assertion of digital sovereignty typically occurs vis-à-vis corporations, not governments. Third, because our lives are 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 towards in different measures), the regulation of the internet almost inevitably involves foreign actors.<sup>132</sup> 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.<sup>133</sup> The EU’s General Data Protection Regulation

---

<sup>130</sup> 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.”).

<sup>131</sup> Lida Ayoubi, *Intellectual Property Commercialisation and Protection of Mātauranga Māori in New Zealand Universities*, 28 N.Z. U. L. R. 521, 553 (2019).

<sup>132</sup> 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).

<sup>133</sup> 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.”).

(GDPR) does not regulate the processing of personal information about a U.S. 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.<sup>134</sup> Anu Bradford labels this the “Brussels Effect.”<sup>135</sup> While David Johnson and David Post famously argued that the global nature of the internet made any sovereign assertion illegitimate,<sup>136</sup> Jack Goldsmith demonstrated that inter-jurisdictional conflicts are not new with the internet, and that international law has tools to manage them.<sup>137</sup> Paul Berman goes further to argue that pluralist approaches to governance should be normatively welcome as they better express contemporary conditions.

Digital sovereignty increasingly means regulating not 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<sup>138</sup> 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 us all to national spaces for commerce and speech, where once we could transact and speak across the world. The specter of the 193 nations of the United Nations, and other sub- and supra-national jurisdictions besides, regulating the internet at the same time seems daunting indeed. Instead of the world’s most free speech zone, the internet may become the world’s most unfree zone, 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

---

<sup>134</sup> 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/> (“we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide”).

<sup>135</sup> 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.”).

<sup>136</sup> 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.”).

<sup>137</sup> See Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

<sup>138</sup> 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.

governance “is largely being mediated by the private parties that hold and manage our data.”<sup>139</sup> “It is these companies that increasingly determine whose rules govern and, in key ways, how they are interpreted and applied,” she writes. Writing about digital sovereignty, Lucien Floridi observes, “The most visible clash is between companies and states.”<sup>140</sup>

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.”<sup>141</sup> Much of the enforcement activity under the GDPR is, accordingly, targeted at corporations. India worries that foreign companies are benefiting from local data—the twenty-first century version of serving as the source of raw materials for the manufacturers of the Global North.

### 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.”<sup>142</sup> 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.”<sup>143</sup>

In *Seeing Like a State*, historian James C. Scott argues that increases in what he calls “legibility” were a critical part of large governmental projects.<sup>144</sup> 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 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<sup>145</sup> can be exploited by the state as well.

---

<sup>139</sup> Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 185 (2018).

<sup>140</sup> See Lucien Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters*, 33 PHIL. & TECH. 369, 371 (2020).

<sup>141</sup> See Tambiana Madiega, *Digital Sovereignty for Europe*, EUROPEAN PARLIAMENTARY RESEARCH SERVICE, 1 (2020), [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

<sup>142</sup> Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).

<sup>143</sup> 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).

<sup>144</sup> JAMES C. SCOTT, *SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED* (1998).

<sup>145</sup> JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 38 (2019).



Scott argues that mid-twentieth century failures of government planning resulted from hubris, with the planners “forgetting that they were mortals and acting as if they were gods.”<sup>146</sup> 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.<sup>147</sup> 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.”<sup>148</sup> Günther Oettinger, then a member of the European Commission for Budget and Human Resources, explained that “The digital single market can be a win-win” for both European and Silicon Valley firms.<sup>149</sup> Andrus Ansip, the European Commissioner for Digital Single Market from 2014-2019, similarly suggested, “The digital single market ”will provide opportunities for trade, investment, innovation not only for Europe, but globally — also, for the United States.”<sup>150</sup> Fredrik Persson, chairman of the Confederation of Swedish Enterprise cautions that European efforts towards digital sovereignty “should not create a European fortress that pulls up the drawbridge to the outside world.”<sup>151</sup> 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.”<sup>152</sup> Many European

---

<sup>146</sup> SCOTT, *supra* note 144, at 342.

<sup>147</sup> *Id.* at 346.

<sup>148</sup> Hamza Shaban, *European Union Unveils Digital Single Market Plan*, BUZZFEED NEWS (May 2015), <https://www.buzzfeednews.com/article/hamzashaban/european-union-unveils-digital-single-market-plan>. See also David O’Sullivan, *Stop the Hysteria: Of course, Europe Wants an Open Internet*, WIRED (2015), <https://www.wired.com/2015/04/eu-ambassador-on-open-internet/>.

<sup>149</sup> Hamza Shaban, *EU Digital Commission to Silicon Valley: Relax*, BUZZFEED NEWS (Sept. 2015), <https://www.buzzfeednews.com/article/hamzashaban/eu-digital-commissioner-to-silicon-valley-relax>.

<sup>150</sup> Hamza Shaban, *Digital Single Market Isn’t Anti-American, Says EU Commissioner*, BUZZFEED NEWS (May 2015), <https://www.buzzfeednews.com/article/hamzashaban/digital-single-market-isnt-anti-american-says-eu-commissione>.

<sup>151</sup> Theodore Christakis, *European Digital Sovereignty* 58 (2020), available at <https://cesice.univ-grenoble-alpes.fr/actualites/2020-12-15/european-digital-sovereignty-successfully-navigating-between-brussels-effect-and-europe-s-quest>.

<sup>152</sup> 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>.

leaders have explicitly disavowed protectionism, instead embracing the coexistence of foreign and domestic technology companies.

Other voices within the European Union, however, portray issues of digital sovereignty as a zero-sum geopolitical struggle. In 2019, French President Emmanuel Macron declared, “The battle we’re fighting is one of sovereignty.” He continued, “If we don’t build our own champions in all new areas — digital, artificial intelligence — our choices ... will be dictated by others.”<sup>153</sup> The European Parliament’s study of digital sovereignty echoes this: “EU policy-makers have identified a potential dependence on foreign technology as presenting a risk to Europe’s influence.”<sup>154</sup> Commissioner Thierry Breton declares that “European data will be used for European companies in priority, for us to create value in Europe.”<sup>155</sup>

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 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, we no longer control our 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.”<sup>156</sup> 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.”<sup>157</sup>

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

---

<sup>153</sup> 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.

<sup>154</sup> European Parliament Think Tank, *Digital sovereignty for Europe (2020)*, available at [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2020\)651992](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)651992).

<sup>155</sup> Quoted in Frances Burwell & Kenneth Propp, *The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World?*, ATLANTIC COUNCIL 1, 6 (2020), <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>.

<sup>156</sup> Foo Yun Chee, *This is the EU’s plan to compete with Silicon Valley*, WORLD ECONOMIC FORUM (Feb. 2020), <https://www.weforum.org/agenda/2020/02/eu-data-market-technology-silicon-valley>.

<sup>157</sup> Quoted in Frances Burwell & Kenneth Propp, *The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World?*, ATLANTIC COUNCIL 1, 6 (2020), <https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf>.

of having ‘10 companies worth €100 billion by 2030’ in Europe ... after he received ... recommendations to encourage the emergence of digital giants in Europe.”<sup>158</sup> Some in the EU wish to create their own “European digital champions.”<sup>159</sup> 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.<sup>160</sup>

### III. The Double-Edged Sword of Digital Sovereignty

Digital sovereignty can grant governments extensive powers over the companies that collect unprecedented amounts of data over us. We examine here a number of ways in which that power can lend itself to abuse. Even well-intentioned law—in the examples here designed to protect against abusive speech, or to protect privacy or national security—can be prone to abuse. We offer examples of this possibility below, noting that these rules can be implemented, interpreted, or enforced in ways that favor powerful politicians.

As much as sovereignty is often necessary for democratic governance, it can also immunize oppression. Louis Henkin acerbically noted that the “most common use of the word ‘sovereignty’ may be in sovereign immunity--immunity from law, immunity from scrutiny, immunity from justice.”<sup>161</sup>

This dual nature may explain what appears to be a double-standard in judging digital sovereignty acts by different countries. That is, the same norm could be used to help ensure that foreign companies protect the rights of local citizens, or it could be used to threaten those foreign companies when they don’t follow the demands of an authoritarian government. For example, when Russia passes a “grounding law” that requires internet companies with more than 500,000 daily visitors to open offices in Russia,<sup>162</sup> that seems distinctly more dangerous<sup>163</sup>

---

<sup>158</sup> 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/>.

<sup>159</sup> See Christakis, *supra* note 26, at 89.

<sup>160</sup> Georgia Wells, Jeff Horwitz and 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.>

<sup>161</sup> See Henkin, *supra* note 20, at 13.

<sup>162</sup> See *Putin Signs Into Law Bill on ‘Grounding’ Google, Facebook, Other IT Giants in Russia*, INTERFAX (July 1, 2021), <https://interfax.com/newsroom/top-stories/72163/>.

<sup>163</sup> See Vittoria Elliott, *New Laws Requiring Social Media Platforms to Hire Local Staff Could Endanger Employees*, REST OF WORLD (May 14, 2021), <https://restofworld.org/2021/social-media-laws-twitter-facebook/#:~:text=Jason%20Pielemeier%2C%20policy%20director%20of,refuse%20to%20take%20government%20orders.>

than European Union obligations for maintaining a local representative.<sup>164</sup> Even the Indian government's demand that Twitter appoint local grievance officers leaves open the possibility of retaliation against such officers for failure to abide government orders.<sup>165</sup> The intermediary rules requiring local grievance officers seem to have been instituted by Prime Minister Narendra Modi's government following its displeasure with Twitter.<sup>166</sup>

### A. Speech

*NetzDG (Germany)*. Germany's Network Enforcement Act of 2018 (popularly known as "NetzDG") requires social media companies with two million or more users to remove "manifestly unlawful" speech within twenty-four hours after user complaint, with limited exceptions. Repeat failures can lead to fines of up to 50 million euros. "In effect, the NetzDG conscripts social media companies into governmental service as content regulators," Diana Lee writes.<sup>167</sup> Germany's broad criminal law related to speech makes this even more risky than it might be elsewhere: "It can be a criminal offense in Germany to call another person a 'jerk,' or even to use the informal du, or 'thou,'" to communicate a lack of respect for the recipient," Lee notes, quoting research by James Whitman.<sup>168</sup> NetzDG specifies 22 offences that require such rapid deletion, including libel, defamation, sedition, and calls for violence. As Lee notes, "In close cases, social media companies will likely err on the side of caution in order to avoid penalties

---

<sup>164</sup> GDPR, art 27 (requiring local representative of foreign data controllers or processors that lack a local establishment).

<sup>165</sup> See Saritha Rai & Upmanyu Trivedi, *Twitter to 'Fully Comply' With India Internet Rules*, BLOOMBERG (July 8, 2021), [https://www.bloomberg.com/news/articles/2021-07-08/twitter-pledges-to-fully-comply-with-india-internet-rules?sref=ExbtjcSG&mc\\_cid=3a6c8a29f1&mc\\_eid=18fe0b3837](https://www.bloomberg.com/news/articles/2021-07-08/twitter-pledges-to-fully-comply-with-india-internet-rules?sref=ExbtjcSG&mc_cid=3a6c8a29f1&mc_eid=18fe0b3837). The rules require three officers, all of whom must be Indian residents: A Chief Compliance Officer "responsible for ensuring compliance" with local legislation and regulation, "a nodal person of contact for 24x7 coordination with law enforcement agencies and officers," and a grievance officer who will be responsible for all functions mentioned under the grievance redressal mechanism. *Modi Govt Announces New Rules to Tighten Oversight Over Social Media, Digital Media Platforms, Streaming Services*, THE WIRE (In.) (Feb. 25, 2021), <https://thewire.in/government/modi-govt-announces-new-rules-to-tighten-oversight-over-social-media-digital-media-platforms-streaming-services>.

<sup>166</sup> Aditya Kalra & Sankalp Phartiyal, *India plans new social media controls after Twitter face-off*, REUTERS, Feb. 24, 2021 10:19 a.m., <https://www.reuters.com/article/us-india-tech-regulation/india-plans-new-social-media-controls-after-twitter-face-off-idUSKBN2AO201>.

<sup>167</sup> Diana Lee, *Germany's NetzDG and the Threat to Online Free Speech*, MEDIA FREEDOM & INFORMATION ACCESS CLINIC (Oct. 10, 2017), <https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech>; <https://law.yale.edu/mfia/case-disclosed?author=24346>

<sup>168</sup> Id. (quoting James Q. Whitman, *Enforcing Civility and Respect: Three Societies*, Yale L. Sch. Fac. Scholarship Series 1293, [http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1650&context=fss\\_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1650&context=fss_papers).)

under the NetzDG.<sup>169</sup> Many worry about the possibility of over-blocking content, given the penalties for non-compliance with the takedown obligation.<sup>170</sup>

By requiring incredibly rapid takedowns, such laws “virtually require the use of upload filters,” as Hannah Bloch-Wehba argues.<sup>171</sup> Bloch-Wehba observes that automated content moderation “preserv[es] the centralization and dominance of large technology companies,” thereby making “surveillance cheaper and easier for law enforcement.”<sup>172</sup> She worries that social media companies will internalize the political goals of enforcers to avoid enforcement actions: “Platforms adapt their content moderation rules and practices to conform to regulators’ preferences, both to comply and to avoid new regulations.”<sup>173</sup> Annemarie Bridy elaborates, worrying about the “troubling dynamic in which platform executives seek to appease government actors—and thereby to avoid additional regulation—by suppressing speech in accordance with the prevailing political winds.”<sup>174</sup>

*Eva Glawischnig-Piesczek v Facebook Ireland Limited (European Union)*. Can an internet company be liable if it refuses to remove a post calling a member of parliament a “corrupt oaf” and a “fascist”?<sup>175</sup> Possibly, according to the Court of Justice of the European Union (CJEU). An Austrian politician had sued Facebook because it had refused to remove a post containing those offensive terms used against her. The case wound its way to the CJEU, which held that the EU’s E-Commerce Directive<sup>176</sup> did not preclude liability on Facebook’s part for refusing to remove this content. The E-Commerce Directive provides protections for “information society services.” Article 15 provides, in part: “Member States shall not impose a general obligation on providers, when providing [information society services], to monitor the information which they transmit or store, nor a general obligation actively to seek facts or

---

<sup>169</sup> *Id.*

<sup>170</sup> Amelie Heldt, *Reading between the lines and the numbers: an analysis of the first NetzDG Reports*, 8(2) INTERNET POLICY REV. 1, 5 (2019), at <http://policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports>.

<sup>171</sup> Hannah Bloch-Wehba, *Automation in Moderation*, 53 CORNELL INT’L L.J. 41, 69 (2020). She notes for example that Google’s NetzDG transparency report “documents how it uses hashing, fingerprinting, and automated flagging technologies to try to identify unlawful content more quickly.” *Id.* at 70.

<sup>172</sup> *Id.* at 46.

<sup>173</sup> *Id.*

<sup>174</sup> Annemarie Bridy, *Moderation’s Excess*, JOTWELL (Mar 27, 2020), <https://cyber.jotwell.com/moderations-excess/>.

<sup>175</sup> The specific terms were “lousy traitor of the people” (“miese Volksverräterin”), “corrupt oaf” (“korrupter Trampel”), and a member of a “fascist party” (“Faschistenpartei”). Luc von Danwitz, *The Contribution of Eu Law to the Regulation of Online Speech the Glawischnig-Piesczek Case and What It Means for Online Content Regulation*, 27 MICH. TECH. L. REV. 167, 171 (2020).

<sup>176</sup> Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.

circumstances indicating illegal activity.” Recital 47 of the E-Commerce Directive, however, permits monitoring obligations in a specific case—such as the one in *Glawischnig-Piesczek*.<sup>177</sup> The CJEU went further to conclude that the Austrian court could order the deletion of the particular post, but also prevent any post with “words having equivalent meaning” across Facebook sites “worldwide.”

The demand to remove posts “having equivalent meaning” across Facebook worldwide seems to require automated systems that are likely to produce significant errors.<sup>178</sup> Even this Article might not pass such a filter! And the decision to allow an Austrian court to order a global removal, in the context of criticism (warranted or not) of a politician, no less, will embolden other states to demand the same. The assertion of Austrian law across the world seems difficult to justify, even more so on matters involving political speech. The CJEU’s sustaining of the Austrian court’s power to order the removal of the post would have been easier to defend if it did not include all “equivalent” posts, and if it was limited to Austria (or perhaps the EU). But the underlying law may make it difficult to call out politicians who are actually corrupt or fascist—because of worries that they may sue.

At the same time, Facebook’s defense in the case that it was governed by either Irish law (because of its European headquarters) or U.S. law (because of its global headquarters), but not Austrian law, was itself an attack on Austrian digital sovereignty, which both Austria and the CJEU properly rebuffed. After all, as long as speech law has not been harmonized across the European Union, to subject Austrians to Irish speech law based on the jurisdictional choices of Facebook would be to do an end-run around Austrian law.<sup>179</sup>

## B. Privacy

*Justice Reform Act (France)*. In 2016, lawyer and machine learning expert, Michaël Benesty, analyzed French asylum decisions by judge, revealing that some judges rejected almost all asylum requests, while others accepted most.<sup>180</sup> The study caused a furor in France, and led to a law that criminalized any such studies, punishable by up to five years in prison.<sup>181</sup> The

---

<sup>177</sup> Felipe Romero Moreno, ‘Upload filters’ and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market, *INT’L REV. L., COMPUTERS & TECH.*, 34:2, 153, 154 (2020).

<sup>178</sup> See Natasha Duarte, Emma Llansó, and Anna Loup, *Mixed. Messages? The Limits of Automated Social Media Content Analysis*, Ctr. for Democracy & Technology (2017); see also Emma Llansó, *No amount of “AI” in content moderation will solve filtering’s prior-restraint problem*, *Big Data & Society* (Jan. 2020).

<sup>179</sup> See ANUPAM CHANDER, *THE ELECTRONIC SILK ROAD* 34 (2013) (arguing that “public policy objectives cannot easily be evaded through a simple jurisdictional sleight of hand or keystroke”).

<sup>180</sup> Malcolm Langford & Mikael Rask Madsen, *France Criminalises Research on Judges*, *VERFASSUNGSBLOG*, June 22, 2019, <https://verfassungsblog.de/france-criminalises-research-on-judges/>.

<sup>181</sup> See *France Bans Judge Analytics, 5 Years in Prison for Rule Breakers*, *ARTIFICIAL LAWYER* (June 4, 2019), <https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison->

new Article 33 of the Justice Reform Act reads: “No personally identifiable data concerning judges or court clerks may be subject to any reuse with the purpose or result of evaluating, analyzing or predicting their actual or supposed professional practices.”<sup>182</sup> Such a law makes it more difficult to scrutinize the judicial process and to identify judges that might be hostile to particular claims.

*Data Protection/Didi (China)*. On June 30, 2021, Didi, the ride-hailing firm based in Beijing, went public on the New York Stock Exchange.<sup>183</sup> On July 2, the Cyberspace Administration of China (“CAC”) announced a cybersecurity review of Didi, and on July 4, it ordered the Didi app removed from Chinese app stores.<sup>184</sup> The cybersecurity review was aimed at “preventing national data security risks, maintaining national security and safeguarding public interests.”<sup>185</sup> CAC ordered the app removal because it found that the app was “illegally collecting and using personal information.”<sup>186</sup> For the cybersecurity review, the CAC relied on the Cybersecurity Law of 2017 and the Measures on Cybersecurity Review issued thereunder in 2020.

Chinese commentators explained the cybersecurity review as being motivated by the “hypothetical scenario of the US coercing Chinese firms to submit data..., citing the US government’s track record of stopping at nothing to forcing businesses to surrender.”<sup>187</sup> A Chinese Foreign Ministry spokesperson lent support to this concern, arguing that “it is the US that forces companies to open ‘back doors’ and illegally obtain user data.”<sup>188</sup> Zuo Xiaodong, the vice-president of the China Information Security Research Institute similarly stated, “In the listing process in the US, some important data and personal information held by Chinese companies may be revealed due to the US regulation request.”<sup>189</sup>

---

[for-rule-breakers/](#). One British commentator observes that “the old law against ‘Scandalising the Judiciary’ was only recently abolished in England & Wales, which shows that judges over here have not always liked to be scrutinised too closely either.” *Id.*

<sup>182</sup> Jason Tasha, *France bans publishing of judicial analytics and prompts criminal penalty*, ABA J., June 7, 2019, 12:51 PM CDT, <https://www.abajournal.com/news/article/france-bans-and-creates-criminal-penalty-for-judicial-analytics> (quoting translation by Rebecca Loescher). See also original text at [https://www.legifrance.gouv.fr/jorf/article\\_jo/JORFARTI000038261761?r=LEGAIP0IBR](https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038261761?r=LEGAIP0IBR).

<sup>183</sup> <https://www.nytimes.com/2021/06/30/technology/didi-wall-street-initial-public-offering.html>.

<sup>184</sup> Zhijing Yu, Vicky Liu & Yan Luo, *China Initiates Cybersecurity Review of Didi ChuXing and Three Other Chinese Mobile Applications*, COVINGTON: INSIDE PRIVACY (July 6, 2021), <https://www.insideprivacy.com/international/china/china-initiates-cybersecurity-review-of-didi-chuxing-and-three-other-chinese-mobile-applications/>.

<sup>185</sup> *Id.*

<sup>186</sup> *Id.*

<sup>187</sup> Li Qiaoyi & Zhang Hongpei, *3 more internet firms scrutinized amid rising data security concern*, GLOBAL TIMES (China), July 5, 2021, 11:28 PM, <https://www.globaltimes.cn/page/202107/1227899.shtml>.

<sup>188</sup> *Id.*

<sup>189</sup> *Id.*

Seen from one angle, the concerns are similar to those expressed by the Court of Justice of the European Union with respect to data transfers to the United States. After all, there the European court cited Executive Order 12333, Section 702 of the Foreign Intelligence and Surveillance Act, and Presidential Policy Directive 28 to argue that U.S. law did not sufficiently protect the data of foreigners from American governmental surveillance.<sup>190</sup> In that sense, the Didi enforcement order could be seen as an effort to protect the personal data of Chinese residents. But at the same time, the Didi enforcement effort, the first application of the cybersecurity review, was also a warning to Chinese companies about who the boss is. In that sense, the enforcement effort could be read, not as an intervention designed to protect Chinese data—after all, personal information is typically not shared as part of any U.S. securities filing—but rather a shot across the bow to multi-billion dollar companies to not tangle with regulators in the future.

### C. National Security

*TikTok Ban (United States)*. On July 31, 2020, President Donald Trump announced on Air Force One that “as far as TikTok is concerned, we’re banning them from the U.S.”<sup>191</sup> A flurry of executive orders would follow. On August 6, 2020, President Trump issued two parallel executive orders targeting TikTok and another Chinese-owned app, WeChat,<sup>192</sup> followed by another order requiring ByteDance, the Beijing-based owner of TikTok, to divest its U.S. TikTok subsidiary following a national security review by the Committee on Foreign

---

<sup>190</sup> Case C-311/18, *Data Prot. Comm'r, v. Facebook Ireland Ltd*, ECLI:EU:C: 2020:559, ¶ 182-84 (July 16, 2020).

<sup>191</sup> Riya Bhattacharjee, Amanda Macias, Jordan Novet, *Trump Says He Will Ban TikTok Through an Executive Action*, CNBC (July 31, 2020), <https://www.cnbc.com/2020/07/31/trump-says-he-will-ban-tiktok-through-executive-action-as-soon-as-saturday.html>.

<sup>192</sup> Executive Order on Addressing the Threat posed by TikTok, Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (“any person or with respect to any party, subject to the jurisdiction of the United States” would be prohibited from transacting with ByteDance Ltd., the Chinese owner of Tik Tok, or any of its subsidiaries); Executive Order on Addressing the Threat posed by WeChat Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020) (order prohibits “any transaction *that is related to WeChat* . . . with TenCent Holdings Ltd., Shenzhen, China, or any subsidiary of that entity . . .”); Pres. Proc. No. 10,061, 84 Fed. Reg. 51,295 (ordering ByteDance to divest all of its rights and interests in any assets or property used to enable or support the operation of TikTok in the United States, and “any data obtained or derived from TikTok or Music.ly application users in the United States” within 90 days.); Press Release, U.S. Dep’t of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States (Sept. 18, 2020), <https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect>; Press Release, U.S. Dep’t of Com., Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States (Sept. 18, 2020), <https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect>.



Investment in the United States (CFIUS).<sup>193</sup> Through TikTok, the President argued, the Chinese government could secretly compile compromising data about Americans, enabling blackmail.<sup>194</sup> The Trump Administration seemed to be relying on a frighteningly broad provision of the Chinese National Intelligence Law, Article 7, which states that “any organization or citizen shall support, assist, and cooperate with state intelligence work according to law.” The Trump Administration also argued that the Chinese government would use the app to censor American speech or to disseminate propaganda. TikTok had indeed been caught suspending an American teenager who cleverly used an eyelash tutorial to criticize the Chinese government’s treatment of Uyghur Muslims.<sup>195</sup> Facing a furor, TikTok apologized for what it described as an error and restored her account. Since that time, posts with the hashtag #uyghur have garnered 82.5 million views on the app.<sup>196</sup>

President Trump announced the TikTok ban some three months before the election, pointing his fingers at an alleged insidious foreign plan to infiltrate the United States. But when federal courts saw the government’s secret evidence against TikTok, they sided with TikTok, preliminarily enjoining the TikTok and WeChat bans.<sup>197</sup> Judge Carl Nichols, a Trump appointee to the federal bench, halted the TikTok ban despite the government’s claims that it posed a national security threat.<sup>198</sup> In a second case, Judge Wendy Beetlestone declared the government’s concerns “hypothetical.”<sup>199</sup> Notably, the CFIUS divestiture order, however, was neither challenged, nor enforced.

The national security rationales conveniently justified actions that targeted a platform that had proved particularly troublesome to the President.<sup>200</sup> Trump borrowed even more of the

---

<sup>193</sup> Pres. Proc. No. 10,061, 84 Fed. Reg. 51,295 (ordering ByteDance to divest all of its rights and interests in any assets or property used to enable or support the operation of TikTok in the United States, and “any data obtained or derived from TikTok or Music.ly application users in the United States” within 90 days.).

<sup>194</sup> *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 77 (D.D.C. 2020).

<sup>195</sup> Paige Leskin, *TikTok issues public apology for suspending the account of the teen behind the viral Chinese takedown video disguised as a makeup tutorial*, BUS. INSIDER, Nov. 2019, <https://www.businessinsider.com/tiktok-apology-china-muslims-viral-video-feroza-aziz-suspend-politics-2019-11>.

<sup>196</sup> Search on TikTok app on May 10, 2021.

<sup>197</sup> *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912, 928 (N.D. Cal. 2020) (“On this limited record, the prohibited transactions burden substantially more speech than is necessary to serve the government’s significant interest in national security, especially given the lack of substitute channels for communication.”).

<sup>198</sup> *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 85 (D.D.C. 2020) (“the specific evidence of the threat posed by Plaintiffs, as well as whether the prohibitions are the only effective way to address that threat, remains less substantial.”).

<sup>199</sup> *Marland v. Trump*, 498 F. Supp. 3d 624, 642 (E.D. Pa. 2020).

<sup>200</sup> Stuart Emmrich, *Is Sarah Cooper the Real Reason Donald Trump Wants to Ban TikTok?*, VOGUE, (August 2020), at <https://www.vogue.com/article/is-sarah-cooper-the-reason-donald-trump-wants-to->

authoritarian internet playbook than might be obvious: like authoritarians everywhere, he sought to silence his critics. TikTok, after all, was the one massive social media platform in the U.S that he had not mastered. If he had banned Twitter, Facebook, or YouTube, he would have lost a channel to reach millions of his followers directly.<sup>201</sup>

In 2021, a new President would revoke the TikTok and WeChat bans, ordering instead a broad review of access to United States' persons sensitive data by foreign adversaries.<sup>202</sup> He said that such a review would be based on "rigorous, evidence-based analysis and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives, including the preservation and demonstration of America's core values and fundamental freedoms."<sup>203</sup> Coupling the rescission of the prior order with this statement suggests that the earlier executive orders failed to meet those standards.

The failure of the TikTok ban is a sign of healthy checks and balances, but the fact that it occurred shows that such checks and balances are necessary. The willingness of federal courts to refuse to meekly accept the President's claim of a national security emergency is heartening. This is also a story of a Congress that had anticipated abuses; courts that enjoined the TikTok and WeChat bans relied in part on the fact that Congress had provided protections for speech from the otherwise broad emergency economic powers that Congress granted to the President.<sup>204</sup>

---

[ban-tik-tok](#). Under this theory, the WeChat ban would be merely collateral damage, as it would be odd to target TikTok without also banning this other popular Chinese-owned app.

<sup>201</sup> <https://www.nbcnews.com/think/opinion/trump-s-facebook-account-should-never-be-reinstated-because-we-ncna1266182> (32 million Facebook followers); <https://www.bbc.com/news/technology-56675272> (90 million Twitter followers); <https://www.youtube.com/channel/UCAqI2DyGU2un1Ei2nMYsqOA> (2.75 million subscribers on frozen YouTube channel).

<sup>202</sup> *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*, June 9, 2021; see Kim Lyons, *Biden Revokes Trump Executive Order That Targeted Section 230*, VERGE (May 15, 2021), <https://www.theverge.com/2021/5/15/22437627/biden-revokes-trump-executive-order-section-230-twitter-facebook-google>. The Biden Administration has not yet withdrawn the CFIUS executive order requiring divestiture, but does not seem to be enforcing that order.

<sup>203</sup> <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/>.

<sup>204</sup> *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 80 (D.D.C. 2020) ("IEEPA's informational-materials limitation deprives the President of authority to regulate or prohibit—'directly or indirectly,' 'regardless of format or medium of transmission,' and 'whether commercial or otherwise'—the importation or exportation of 'informational materials.'") (citing 50 U.S.C. § 1702(b)(3)); *Marland v. Trump*, 498 F. Supp. 3d 624, 637 (E.D. Pa. 2020) ("With the Berman Amendment, however, Congress modified IEEPA to expressly 'exempt the regulation of informational materials from the Executive's congeries of powers.'") (citation omitted). Judge Laurel Beeler relied on the First Amendment to protect against possible executive overreach, concluding, "On this limited record, the prohibited transactions burden substantially more speech than is necessary to serve the government's significant interest in national

*NSO Spyware for Hire (Israel)*. In July 2021, Amnesty International revealed that some 50,000 individuals in more than 45 countries—including fourteen heads of state<sup>205</sup> and numerous journalists—were the target of phone hacking, using software sold by the NSO Group.<sup>206</sup> For example, an “investigation suggests the Hungarian government of Viktor Orbán appears to have deployed NSO’s technology as part of his so-called war on the media, targeting investigative journalists in the country as well as the close circle of one of Hungary’s few independent media executives.”<sup>207</sup>

NSO is hardly the only Western company implicated in the sale of repressive technologies. The Israeli company Cellebrite has been implicated in oppression by governments across the world, but still is planning an IPO in New York.<sup>208</sup> Its IPO prospectus warns investors that its “solutions may be used by customers in a way that is, or that is perceived to be, incompatible with human rights.”<sup>209</sup> Another Israeli “hacking-for-hire” firm, Candiru, has “helped government clients spy on more than 100 victims around the world, including politicians, dissidents, human rights activists, embassy workers and journalists,” at least according to Microsoft.<sup>210</sup> The Israeli company Verint Systems reportedly sold spying tools to

---

security, especially given the lack of substitute channels for communication.” *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912, 928 (N.D. Cal. 2020).

<sup>205</sup> Peter Beaumont and Philip Oltermann, *Israel to examine whether spyware export rules should be tightened*, GUARDIAN (July 22, 2021, 11:45 EDT), <https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus>.

<sup>206</sup> Stephanie Kirchgaessner et al., *Revealed: leak uncovers global abuse of cyber-surveillance weapon*, GUARDIAN (July 18, 2021, 12:00 EDT), <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>.

<sup>207</sup> See Stephanie Kirchgaessner et al., *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon*, GUARDIAN (July 18, 2021), <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>.

<sup>208</sup> See *Open Letter: Cellebrite should not go public without demonstrating human rights compliance*, ACCESS NOW (July 13, 2021), [https://www.accessnow.org/cms/assets/uploads/2021/07/CSO\\_Open-Letter\\_on\\_Cellebrite.pdf](https://www.accessnow.org/cms/assets/uploads/2021/07/CSO_Open-Letter_on_Cellebrite.pdf); See Avi Asher-Schapiro, *Israeli Surveillance Firm’s Nasdaq Plans Challenged by Digital Rights Groups*, REUTERS (July 13, 2021), <https://www.reuters.com/article/tech-business-surveillance/israeli-surveillance-firms-nasdaq-plans-challenged-by-digital-rights-groups-idUSL8N20O5IP>.

<sup>209</sup> Cellebrite, Inc., Registration Statement June 29, 2021 at 26.

<sup>210</sup> *Fighting Cyberweapons Built by Private Businesses*, MICROSOFT (July 15, 2021), <https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/>; Bill Marczak et al., *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*, CITIZEN LAB (July 15, 2021), <https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/>.

Azerbaijan that were used to identify its citizens' sexual orientations through Facebook, and to Indonesia to collect personal information about LGBT rights activists.<sup>211</sup>

This is not a problem of Israeli exporters alone. In 2015, the Italian company, Hacking Team, was itself hacked, revealing an extensive client list in authoritarian governments, including governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE.<sup>212</sup> The U.S. networking equipment company Sandvine reportedly supplied an Internet-blocking technology to Belarus that was used to block access to websites and repress protests during the 2020 Belarussian elections.<sup>213</sup> Furthermore, NSO's exports themselves implicate the laws of EU member states Bulgaria and Cyprus, as NSO exports its products from those countries as well.<sup>214</sup>

Western commentators rightly point out that Chinese technology companies often sell their technologies to repressive governments across Africa and elsewhere. They go on to distinguish a liberal Western approach to technology from a repressive Chinese approach.<sup>215</sup> But why use Chinese surveillance technology when you can buy Western technology that will get the job done?<sup>216</sup> And this argument seems to forget that it was Western companies that helped build China's Great Firewall of China in the first instance.<sup>217</sup>

---

<sup>211</sup> Jason Murdock, *Israeli Companies Sold Surveillance Tech and Knowledge Used for Persecuting Dissidents, Journalists, LGBT People*, NEWSWEEK, 10/19/18, <https://www.newsweek.com/israeli-companies-sell-surveillance-tech-and-knowledge-used-persecuting-1178084>.

<sup>212</sup> Alex Hern, *Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim*, GUARDIAN (July 6, 2015 07:46 EDT), <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim>.

<sup>213</sup> <https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers>.

<sup>214</sup> Amnesty International, Privacy International and The Centre for Research on Multinational Corporations, *Operating from the Shadows: Inside NSO Group's Corporate Structure* 7 (2021).

<sup>215</sup> See, e.g., State Department, *The Elements of the China Challenge* 17 (2020) ("Beijing provides digital technology and physical infrastructure to advance the CCP's authoritarian objectives throughout the [Indo-Pacific] region"); Alina Polyakova and Chris Meserole, *Exporting digital authoritarianism* 5-6 (Brookings) (2019), at [https://www.brookings.edu/wp-content/uploads/2019/08/FP\\_20190826\\_digital\\_authoritarianism\\_polyakova\\_meserole.pdf](https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf).

<sup>216</sup> Cf. Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, For. Aff. (April 8, 2021) (observing that while countries from Ecuador to Kyrgyzstan have "adopted Chinese surveillance technology," "the United States and its tech companies also have a checkered history with the very ideals they claim to uphold.")

<sup>217</sup> According to one report, "China relied on two U.S. companies--Cisco Systems and Juniper Networks--to help carry out its network upgrade, known as "CN2," in 2004. This upgrade significantly increased China's ability to monitor Internet usage. Cisco also sold several thousand routers used to censor web content, and 'firm's engineers have helped set it to spot 'subversive' key-words in messages.'" Robert McMahon and Isabella Bennett, *U.S. Internet Providers and the 'Great Firewall of China'*, Council on Foreign Relations, February 23, 2011 7:00 am (EST), <https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china>.

Israeli law requires exports of such spyware to be approved by its Defense Department, and NSO claims to have received the necessary permits.<sup>218</sup> The NSO spyware scandal reveals the importance of governments regulating not only foreign companies, but also domestic companies, to ensure that these companies do not help infringe human rights elsewhere. A former Cellebrite employee notes that other employees would justify the sales on the ground that “governments could buy the same services from China, therefore better that we sell it to them instead.”<sup>219</sup> But this reasoning would allow one to sell the most deadly services in the world, as long as someone else was selling them too. Furthermore, buying surveillance services from a democratic country may draw less scrutiny than buying services from companies in authoritarian states. Finally, the argument ignores the possibility of jointly pressuring foreign governments to stop permitting their companies to sell such services in the global markets.

## Conclusion

On May 15, 2000, French plaintiffs accused internet pioneer Yahoo! of American imperialism because Yahoo.com made Nazi materials accessible to people across the world.<sup>220</sup> Yahoo!’s lawyers responded that to apply French law to a site based in the U.S. more closely resembled French imperialism.<sup>221</sup> The French court carefully tailored its order to only require Yahoo! to desist from providing the prohibited materials within France. Today, countries across the world have adopted the French position to insist that foreign companies comply with local law, at least on matters significant to them.<sup>222</sup>

A quarter of century after the birth of the global internet, neither the libertarian wishes of early internet pioneers nor the globalist desire for a single global community have prevailed. Instead, we see increasing efforts by the countries of the world to gain control over the internet. This is understandable. As Andrew Woods observes, “states remain the single greatest source of legitimate rules for different peoples with varied community values and experiences on a diverse planet.”<sup>223</sup> Digital sovereignty is simultaneously necessary and scary—necessary to ensure that ordinary laws follow us as we move increasingly online, disciplining the corporations that govern

---

<sup>218</sup> Defense Export Control Law (Israel).

<sup>219</sup> See also Anonymous, *I Worked at Israeli Phone Hacking Firm Cellebrite. They Lied to Us*, Haaretz, July 27, 2021, at <https://www.haaretz.com/israel-news/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us-1.10041753>.

<sup>220</sup> See Greg Wrenn, *Yahoo! V. Licra*, Comm. Law., Fall 2006, at 5, 6.

<sup>221</sup> *Id.*

<sup>222</sup> This does not mean that a foreign court will necessarily enforce such an order, however. In the Yahoo! case, District Judge Fogel, we believe properly concluded, “Although France has the sovereign right to regulate what speech is permissible in France, this Court may not enforce a foreign order that violates the protections of the United States Constitution by chilling protected speech that occurs simultaneously within our borders.” *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L’Antisemitisme*, 169 F. Supp. 2d 1181, 1192 (N.D. Cal. 2001), *rev’d*, 379 F.3d 1120 (9th Cir. 2004), *on reh’g en banc*, 433 F.3d 1199 (9th Cir. 2006), and *rev’d and remanded*, 433 F.3d 1199 (9th Cir. 2006).

<sup>223</sup> Woods, *supra* note 16, at 369.

our work, school, and private lives—but scary because regulation of the internet gives governments even more power to invade broader spheres of our lives. Just as the power wielded by digital corporations must be carefully regulated, so must the power of digital regulators.