Vanderbilt Journal of Transnational Law

Volume 55
Issue 2 *March 2022*

Article 2

3-2022

Sovereignty 2.0

Anupam Chander
Georgetown University

Haochen Sun
University of Hong Kong

Sovereignty 2.0

Anupam Chander & Haochen Sun***

ABSTRACT

Digital sovereignty—the exercise of control over the internet—is the ambition of the world's leaders, from Australia to Zimbabwe, seen as a bulwark against both foreign states and foreign corporations. Governments have resoundingly answered first-generation internet law questions of who, if anyone, should regulate the internet. The answer: they all will. Governments now confront second-generation questions—not whether, but how to regulate the internet. This Article argues that digital sovereignty is simultaneously a necessary incident of democratic governance and democracy's dreaded antagonist. As international law scholar Louis Henkin taught, 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 through careful checks and balances.

TABLE OF CONTENTS

I. INTRODUCTION 284
II. FROM HOBBES TO ZUCKERBERG: THE RISE OF DIGITAL SOVEREIGNTY 290
A. *Defining "Digital Sovereignty"* 291
B. *China: Inventing Digital Sovereignty* 293
C. *The EU: Embracing Digital Sovereignty* 298
D. *Russia: Promoting the Runet* 300
E. *The United States: Digital Sovereignty by Default* . 301
F. *The Global South: Avoiding Data Colonialism* 303
III. HOW DIGITAL SOVEREIGNTY IS DIFFERENT 305

---

* Scott K. Ginsburg Professor of Law and Technology, 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. We are also grateful to excellent editing by *Vanderbilt Journal of Transnational Law* editors Lauren Donnelly, Christina McLaughlin, Joshua Moscow, and others.

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

A. *Always Global* 306
B. *Against Corporations* 307
C. *More Control* 308
D. *Enables Protectionism* 309
IV. THE DOUBLE-EDGED SWORD OF DIGITAL SOVEREIGNTY 311
A. *Speech* 312
1. NetzDG (Germany). 312
2. Eva Glawischnig-Piesczek v Facebook Ireland Limited (European Union). 314
B. *Privacy* 315
1. Justice Reform Act (France). 315
2. Data Protection/Didi (China) 316
C. *National Security* 317
1. TikTok Ban (United States). 317
2. NSO Spyware for Hire (Israel). 320
V. CONCLUSION 323

I. 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.[1] Sovereignty would prove impossible over a world of bits, with the internet simply routing around futile controls.[2] But reports of the death of sovereignty over the internet proved premature. Consider recent events:

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

1. *See* John P. Barlow, *The Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (July 16, 2021, 1:59 PM), https://www.eff.org/cyberspace-independence [https://perma.cc/JG36-5LNE] (archived Jan. 5, 2022).

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

3. Lily Kuo, *'Jack Ma is Tamed': How Beijing Showed Tech Entrepreneur Who is Boss*, GUARDIAN (Nov. 4, 2020), https://www.theguardian.com/business/2020/nov/04/jack-ma-ant-group-is-tamed-social-media-reacts-after-china-blocks-ipo [https://perma.cc/R58H-RUSF] (archived Jan. 5, 2022).

4. *Id.*

an order to negotiate with news publishers to compensate them for displaying snippets of the publishers' news items before linking to them.[5]

- In July 2021, Luxembourg's privacy regulator fined Amazon $887 million for data protection violations.[6]
- European Union (EU) authorities are simultaneously investigating Google's ad technology, Apple's App Store, Facebook's Marketplace, and Amazon's use of data from its third-party sellers.[7] Even Facebook Dating receives unwanted attention from the British competition authority.[8]
- The technology giants are not safe even at home, as Ant discovered. In the home of most of the world's largest internet companies, the US Federal Trade Commission (FTC) seeks to compel Facebook to divest WhatsApp and Instagram, while investigating Amazon for competing with merchants that use its platform.[9] The federal

---

5. *See* Gaspard Sebag, *Google Told to Pay for News With Ultimatum and $593 Million Fine*, BLOOMBERG (July 13, 2021), https://www.bloomberg.com/news/articles/2021-07-13/google-said-to-be-fined-593-million-by-french-antitrust-agency?sref=CrGXSfHu [https://perma.cc/33FL-7YGP] (archived Jan. 5, 2021).

6. *See* Taylor Telford, *E.U. Regulator Hits Amazon with Record $887 Million Fine for Data Protection Violations*, WASH. POST (July 30, 2021), https://www.washingtonpost.com/business/2021/07/30/amazon-record-fine-europe/ [https://perma.cc/8XE6-3A45] (archived Jan. 5, 2021). The previous highest fine issued by the Luxembourg data protection authority was 18,000 euros. GDPR ENFORCEMENT TRACKER, https://www.enforcementtracker.com/ (last visited Aug. 2, 2021, at 7:35 pm) [https://perma.cc/WS34-ZTCS] (archived Jan. 9, 2022).

7. *See* Sam Schechner & Parmy Olson, *Google Faces EU Antitrust Probe of Alleged Ad-Tech Abuses*, WALL ST. J. (June 22, 2021), https://www.wsj.com/articles/google-faces-eu-antitrust-probe-of-alleged-ad-tech-abuses-11624355128 [https://perma.cc/24CD-PWZ5] (archived Jan. 5, 2021); 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/ [https://perma.cc/9RUJ-F85R] (archived Jan. 5, 2022); Adam Satariano, *Facebook Faces Two Antitrust Inquiries in Europe*, N.Y. TIMES (June 4, 2021) https://www.nytimes.com/2021/06/04/business/facebook-eu-uk-antitrust.html [https://perma.cc/A79B-L5EJ] (archived Jan. 5, 2020); 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 [https://perma.cc/7XK7-7DN6] (archived Jan. 5, 2022).

8. *See* Press Release, U.K. Competition & Mkts. Auth., CMA Investigates Facebook's Use of Ad Data (June 4, 2021), https://www.gov.uk/government/news/cma-investigates-facebook-s-use-of-ad-data [https://perma.cc/FC3W-BYQZ] (archived Mar. 20, 2022).

9. Press Release, Fed. Trade Comm'n, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology [https://perma.cc/NKU5-EHTT] (archived Jan. 5, 2022) (tech in general and the FTC); *Factbox: How Big Tech is Faring Against U.S. Lawsuits and Probes*, REUTERS (Dec. 7, 2021), https://www.reuters.com/technology/big-tech-wins-two-battles-fight-with-us-antitrust-enforcers-2021-06-29/ [https://perma.cc/T4AQ-FTSK] (archived Jan. 23, 2022); *see* Brent Kendall, *Amazon Seeks Recusal of FTC Chairwoman Lina Khan in*

government and all but two US states are bringing antitrust claims against Google,[10] and the US Justice Department is investigating Apple's App Store.[11]

- Assertions of digital sovereignty are hardly limited to Western nations. After Twitter deleted the Nigerian president's tweets warning of a new civil war, the Nigerian government in June 2021 simply banned Twitter from the country. On the eve of an election in January 2021, Uganda went even further, ordering a complete shutdown of the internet, with President Yoweri Museveni explaining that Facebook had deleted pro-government accounts as manipulative.[12] Uganda followed the example of Zimbabwe, which responded to anti-government protests in 2019 by shuttering the internet.[13]

The state (both nation-state as well as nearly every US state) strikes back.[14]

Scholars are sharply divided about the increasing assertion of what is called variously "data sovereignty" or "digital sovereignty."[15]

Antitrust Investigations of Company, WALL ST. J. (June 30, 2021), https://www.wsj.com/articles/amazon-seeks-recusal-of-ftc-chairwoman-lina-khan-in-antitrust-investigations-of-company-11625067962 [https://perma.cc/7UYT-DJKD] (archived Jan. 5, 2022).

10. *See* Press Release, Dep't of Justice, Justice Department Sues Monopolist Google For Violating Antitrust Laws (Oct. 20, 2020), https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws [https://perma.cc/F8M8-NKFA] (archived Jan. 5, 2022) (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 [https://perma.cc/48XM-J94Q] (archived Jan. 27, 2022) (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 [https://perma.cc/939B-LZQ8] (archived Jan. 27, 2022).

11. *See* Leah Nylen, *Apple's Easy Fide from U.S. Authorities May be Over*, POLITICO (June 24, 2020), https://www.politico.com/news/2020/06/24/justice-department-anti-trust-apple-337120 [https://perma.cc/T3DF-7ECC] (archived Jan. 5, 2022) (Apple); *Factbox: How Big Tech is Faring Against U.S. Lawsuits and Probes*, *supra* note 9.

12. *See* Stephen Kafeero, *Uganda Has Cut Off Its Entire Internet Hours to Its Election Polls Opening*, QUARTZ AFRICA (Jan. 13, 2021), https://qz.com/africa/1957137/uganda-cuts-off-internet-ahead-of-election-polls-opening/ [https://perma.cc/J8JY-FZ88] (archived Jan. 5, 2022).

13. *See Zimbabwe Imposes Internet Shutdown Amid Crackdown on Protests*, AL JAZEERA (Jan. 18, 2019), https://www.aljazeera.com/news/2019/1/18/zimbabwe-imposes-internet-shutdown-amid-crackdown-on-protests [https://perma.cc/YVE4-6D7K] (archived Jan. 5, 2022).

14. For a round-up of some recent enforcement actions faced by the biggest technology companies, *see* Joe Panettieri, *Big Tech Antitrust Investigations: Amazon, Apple, Facebook and Google Updates*, CHANNELE2E (Dec. 24, 2021), https://www.channele2e.com/business/compliance/big-tech-antitrust-regulatory-breakup-updates/ [https://perma.cc/VU6J-KPSG] (archived Jan. 5, 2022).

15. We explore various definitions of the terms in Part II, A below.

Some scholars see it as a natural extension of traditional Westphalian sovereignty to the twenty-first century.[16] 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.[17] Other scholars, however, worry that data sovereignty will break the web apart, jeopardizing its numerous global benefits.[18] 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."[19]

Digital sovereignty is necessary 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 review. Away with the "S-word," the preeminent human rights theorist Louis Henkin cautioned.[20] This Article argues that Henkin's concern is even graver with respect to digital sovereignty, which presents a 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 its own citizens, and thus deserves exacting scrutiny. This is the double-edged sword of digital sovereignty: it both enables the protection of residents and their control.

The ongoing tech wars between the United States and China, as this 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

---

16. *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).

17. *See* Renata Avila Pinto, *Digital Sovereignty or Digital Colonialism*, 27 SUR - INT'L J. HUM. RTS. 15, 23–24 (2018); Nick Couldry & Ulises A. Mejias, *Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject*, 20 TELEVISION & NEW MEDIA 336, 337 (2019); *cf.* JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 51 (2019) (noting the distributive nature of the construction of a "biopolitical public domain," where raw data is a resource to be processed).

18. *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.").

19. *Id.* at 1409.

20. *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").

operations in the United States on national security grounds.[21] While dealing with potential threats posed 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.[22] The upshot was that more than 100 million US users[23] 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.[24] American courts reacted to the dark side of the US government's assertions of digital sovereignty. The courts 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."[25]

This Article is the first comprehensive account of digital or data sovereignty.[26] It surveys the various ways in which states are asserting

---

21. *See* Anupam Chander, *Protecting the Global Internet from Technology Cold Wars*, COMMC'NS OF THE ACM 22 (Sept. 2021).

22. *See* Eva Galperin, David Greene, & Kurt Opsahl, *TikTok Ban: A Seed of Genuine Security Concern Wrapped in a Thick Layer of Censorship*, ELEC. FRONTIER FOUND. (Aug. 4, 2020), https://www.eff.org/zh-hant/deeplinks/2020/08/tiktok-ban-seed-genuine-security-concern-wrapped-thick-layer-censorship [https://perma.cc/EAA4-6EXP] (archived Jan. 6, 2022) ("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 [https://perma.cc/B5YM-UHTM] (archived Jan. 6, 2022) (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 [https://perma.cc/VR2S-AAJU] (archived Jan. 14, 2022) (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").

23. 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 [https://perma.cc/23A7-572X] (archived Jan. 6, 2022) ("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.").

24. *See* Taylor Lorenz, *This Is Why You Heard About TikTok So Much in 2020*, N.Y. TIMES (Feb. 26, 2021), https://www.nytimes.com/2020/12/31/style/tiktok-trends-2020.html [https://perma.cc/D4L9-MCCH] (archived Jan. 9, 2022) (discussing how TikTok transformed business, entertainment, news, activism and social connection in 2020).

25. U.S. WeChat Users All. v. Donald J. Trump, 488 F. Supp. 3d 912, 928 (N.D. Cal. 2020); *see also* TikTok Inc. v. Donald J. Trump, President of the United States, 490 F. Supp. 3d 73 (D.D.C. 2020).

26. *Cf.* Woods, *supra* note 16 (arguing that national attempts to regulate the global cloud are legitimate and can be reasonably disciplined through judicial doctrines of sovereign deference); Jennifer Daskal, Borders and Bits, 71 VAND. L. REV. 179, 179 (2018); Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHIL. & TECH. 369, 375 (2020) (arguing that "the best answer to the multinationals' control of the digital is probably the establishment of a (*de jure*

digital sovereignty. It argues that digital 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 also that digital sovereignty is especially susceptible to hijacking by abusive governments.

This 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.[27] 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 disparity 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 sometimes only the negative end of digital regulations can be seen. The American government, academics, 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 aspects of these laws that protect citizens' rights are not recognized as such. Notably, China has been actively protecting citizens' data privacy rights through waves of legislative proposals, regulatory measures, and judicial decisions (though there are dangers in this exercise as observed below[28]).

This Article's argument exposes a difficulty in one popular framing of digital sovereignty as an effort to thwart Chinese technology

---

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 (Dec. 2020) (e-book published by the Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098 [https://perma.cc/Q9ER-8JY9] (archived Jan. 14, 2022).

27. 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 OP. (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 [https://perma.cc/FMA5-NEX5] (archived Jan. 7, 2022). 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/ [https://perma.cc/77QK-NAMT] (archived Jan. 7, 2022); *Timeline of SIM Card Registration Laws*, PRIVACY INT'L (Apr. 21, 2021), https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws [https://perma.cc/9ZAU-CG44] (archived Jan. 7, 2022).

28. *See infra* notes 83–90 and accompanying text.

dominance on the grounds that Chinese technology inherently promotes greater authoritarian controls. This Article agrees that technologies are never neutral,[29] and they can be more or less adaptable for authoritarian purposes. However, this framing of an ethical North vs. an 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 spyware by Israeli surveillance provider NSO dramatize this concern.[30] There is no need for a government to adopt Chinese technologies[31] if one can buy spyware off the shelf from Western suppliers.

This Article argues 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 II describes the emergence of Sovereignty, 2.0. Part III observes the unique characteristics of this new twenty-first-century sovereignty. Part IV explores the double-edged sword of digital sovereignty through recent regulatory interventions. Part V concludes.

II. FROM HOBBES TO ZUCKERBERG: THE RISE OF DIGITAL SOVEREIGNTY

When Thomas Hobbes imagined an "Artificial Man" in the form of a state,[32] 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 daily life. Increasingly, governments across the world have sought to bring these companies under their control. While China pioneered data sovereignty, it is now the demand of governments from Australia to Zimbabwe. The era of countries unsure whether they had the power to regulate the internet is over.

After defining digital sovereignty, this Article reviews below the effort to attain data sovereignty in a few key jurisdictions. The review

---

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

30. *See infra* notes 215–30 and accompanying text.

31. *See* Paul Mozur, Jonah M. Kessel, & Melissa Chan, *Made in China, Exported to the World: The Surveillance State*, N.Y. TIMES (Apr. 24, 2019), https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html. [https://perma.cc/4KZX-7VGL] (archived Jan. 9, 2022).

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

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.

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.[33] 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."[34] The tension between the notion of "digital sovereignty" and the territorial foundation for sovereignty disappears when one recognizes that in order to exercise control over any territory, it is increasingly necessary to exercise control over the online activities available in that territory. This insight connects place and cyberspace.

Woods writes that, in order to control data within their borders to the exclusion of other states, "states can command considerable control over the internet if only because they control the physical components of the network within their borders" through "an impressive arsenal of tools."[35] 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.[36] 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").[37] It seems

---

33. 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."

34. Woods, *supra* note 16, at 360.

35. *Id.* at 360–61.

36. Dan Svantesson, A Starting Point for Re-thinking 'Sovereignty' for the Online Environment (May 10, 2021) (unpublished manuscript) (on file with author).

37. Woods, *supra* note 16, at 364.

clear that multiple states are able to order the same firm how to operate, with occasional conflicts in approaches.[38]

Ke Xu divides sovereignty in cyberspace into three layers: the physical layer (sovereignty over physical internet infrastructure and activities), the code layer (sovereignty over domain names, internet standards, and regulations), and the data layer.[39] 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,"[40] and then extends this to "digital sovereignty," which he defines as the "control of data, software (e.g., AI), standards and protocols (e.g., 5G, domain names), processes (e.g., cloud computing), hardware (e.g., mobile phones), services (e.g., social media, e-commerce), and infrastructures (e.g., cables, satellites, smart cities)."[41]

Data sovereignty, as argued by Paul Rosenzweig, may also be framed as a question: Which sovereign controls the data?[42] The core issue is one of jurisdiction, which is, of course, complicated by the borderless nature of the internet.[43] "In short, the question is: 'Whose law is to be applied?'"[44] 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.'"[45] 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.

This Article will use the term "digital sovereignty" to mean the application of traditional state sovereignty over the online domain, [46] or simply "sovereignty in the digital age."[47] Digital sovereignty should be defined broadly to cover a state's sovereign power to regulate not

---

38. 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. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

39. Ke Xu, *Data Security Law: Location, Position and Institution Construction*, 3 BUS. & ECON. L. REV. 52, 57 (2019).

40. Floridi, *supra* note 26, at 371.

41. *Id.* at 370–71.

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

43. *See id.*

44. *Id.* at 422.

45. *Id.*

46. This accords with the French Senate investigatory committee report, which defines digital sovereignty as the "capacity of the state to act in cyberspace." LE DEVOIR DE SOUVERAINETÉ NUMÉRIQUE: NI RÉSIGNATION, NI NAÏVETÉ, SENAT (2019), http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2019/2019_Infographies/20191004_infog_Souverainete_numerique_021019.pdf [https://perma.cc/9HJR-MGTW] (archived Jan. 14, 2022) (translated by authors)

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

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. The Article uses 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:[48]

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

It is possible to draw a distinction between "data sovereignty" and "digital sovereignty," where "data sovereignty" refers to control over data, including through data protection law, competition law, and national security law. This definition would make data sovereignty a subset of digital sovereignty. But the relationship between "data sovereignty" thus defined and broader issues such as content moderation becomes quickly evident and difficult to disentangle. Stopping information from flowing across borders, for example, implicates speech and commerce, as well as data governance. Indeed, a distinction between dominion over "data" and dominion over the "digital" is hard to sustain. This Article largely uses the term "digital sovereignty" in this paper, recognizing that the term is sometimes used distinctly with "data sovereignty" and sometimes interchangeably.

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, which has been described as "a far-ranging attempt to harness emerging information technologies for policing."[49] Henry Gao observed that Chinese digital sovereignty evolved through different phases—physical controls and then controls over the software layer and

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

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

content.[50] In other words, it went up the internet stack.[51] As James Fallows wrote in a classic Western account of "the Great Firewall of China," "[i]n China, the Internet came with choke points built in."[52] China takes a multifaceted approach to exerting digital sovereignty, which includes controlling its physical infrastructure, regulating content, balancing negative economic impacts, and building international support for its conception of digital sovereignty.[53] 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.[54] However, sometimes the firewall causes collateral impact on internet freedom beyond China's borders through domain name system pollution, where Chinese domain name servers accidentally serve foreign users, thus inadvertently blocking access to websites by users in other countries.[55]

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."[56] 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 the internal affairs of foreign countries.[57] 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

---

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

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

52. James Fallows, *The Connection Has Been Reset*, ATLANTIC (Mar. 2008), https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/ [https://perma.cc/4DX4-XY2X] (archived Jan. 9, 2022).

53. Anqi Wang, *Cyber Sovereignty at Its Boldest: A Chinese Perspective*, 16 OHIO ST. TECH. L.J. 395, 403 (2020); *Protecting Internet Security*, CHINA.ORG, http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm (last visited Jan. 14, 2022) [https://perma.cc/96B7-3ZNQ] (archived Jan. 9, 2022).

54 . *See* Wang, *supra* note 53, at 408, 439.

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

56. *See* Wang, *supra* note 53, at 397.

57. *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").

policies on the internet, and to participate on an equal basis in the governance of international cyberspace—avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries."[58]

China escalated the tech cold war. The Cybersecurity Administration of China opened investigations into the data transfer practices of Chinese tech giant Didi immediately following that company's New York Stock Exchange listing. It then ordered Didi removed from Chinese app stores.[59] Even though Didi's stock price plummeted, Chinese media celebrated the "rise of data sovereignty."[60]

China's conception of digital sovereignty is rooted, Anqi Wang wrote, in traditional notions of territorial sovereignty[61] and officially justified by concern for national and ideological security.[62] China supports a "state-centric multilateralism" model of internet governance, [63] which holds that states, not private sector actors like the Internet Corporation for Assigned Names and Numbers (ICANN), should be driving internet governance.[64] In contrast, the "bottom-up multi-stakeholderism" subscribed to by the United States and other Western countries[65] holds that the private sector and civil society should remain key players in internet governance.[66] The Western "information freedom" approach to the internet[67] is perceived as a threat to "Chinese ideological security" and a tool of cultural

---

58. *See* Wang, *supra* note 53, at 397; Franz-Stefan Gady, *The Wuzhen Summit and the Battle Over Internet Governance*, DIPLOMAT (Jan. 14, 2016), https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/; Bruce Sterling, *Respecting Chinese and Russian Cyber-Sovereignty in the Formerly Global Internet*, WIRED (Dec. 22, 2015), https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in- the-formerly-global-internet/ [https://perma.cc/K743-B5VD] (archived Jan.9, 2022).

59. *See* Jacky Wong, *Didi and the Big Chill on China's Big Data*, WALL ST. J. (July 5, 2021), https://www.wsj.com/articles/didi-and-the-big-chill-on-chinas-big-data-11625479452 (subscription required) [https://perma.cc/R7W4-S6D4] (archived Jan. 9, 2022).

60. *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 [https://perma.cc/YFE5-ECH5] (archived Jan. 9, 2022) ("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.").

61. *See* Wang, *supra* note 53, at 397.

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

63. *Id.* at 443–44.

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

65. *Id.* at 399.

66. *See id.* at 444.

67. *Id.* at 400.

imperialism.[68] The Chinese government instead seeks to use the internet to consolidate party control, maintain social order, and proliferate desirable socialist and Confucian values such as "'patriotism,' 'loyalty to the communist party,' 'dedication to one's work,' 'honesty,' [and] 'filial piety,'" to "develop a cohesive, socialist nation."[69] 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."[70]

China sees US internet infrastructure hegemony as a threat to its digital sovereignty.[71] In 2016, President Xi stated, "the fact that [the internet's] core technology is controlled by others is our greatest hidden danger."[72] Accordingly, the government has been investing heavily in research and development of internet technology[73] and "territorializing critical infrastructure"[74] to escape Western technical and physical network dependence. Part of this effort has been a proliferation of Critical Information Infrastructure (CII) regulations,[75] including data localization regulations through the 2017 Cybersecurity Law (CSL).[76] Not only does Article 37 of the CSL require that data and personal information originating in China be stored within China, but critical information infrastructure operators must also undergo "security assessments" before that data can be transferred abroad.[77] (The first such security assessment—against the ride-hailing company Didi—is described below.[78])

---

68. *Id.* at 406.

69. *Id.* at 407.

70. *Xi Jinping Gives Speech at Cybersecurity and Informatization Work Conference*, CHINA COPYRIGHT & MEDIA (Apr. 19, 2016), https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/ [https://perma.cc/JH49-FMJM] (archived Jan. 9, 2022).

71. *See* Wang, *supra* note 53, at 404–05 (explaining that China perceives US corporate and civil society control over domain names and US-made infrastructure as favoring US interests).

72. *Id.* at 405.

73. *See id.* at 434, 436.

74. *Id.* at 435.

75. *See id.* at 436–37.

76. *See id.* at 408, 456.

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

78. See *infra* notes 191–98 and accompanying text.

Content regulation and censorship is another integral component of China's "information sovereignty" on the internet.[79] Though China's approach to content regulation is more extreme than in other countries,[80] it rejects accusations that its cyber sovereignty policies simply mask authoritarian control.[81] Instead, the government claims to censor "subversive," "harmful," "obscene," or "malicious" content while welcoming "kind criticism."[82] 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."[83] 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."[84]

Some of the measures China takes to regulate content and maintain a "clear cyberspace"[85] include blocking virtual private network (VPN) access, algorithms that divert searches, the Real Name Registration Policy,[86] 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.[87] However, standards for what information is "erroneous" or in violation of the law remain unclear.[88] 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.[89] 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.[90]

---

79. *See* Wang, *supra* note 53, at 452.

80. *See id.* at 466.

81. *See id.* at 416.

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

83. Elsa Kania, Samm Sacks, Paul Triolo, & Graham Webster, *China's Strategic Thinking on Building Power in Cyberspace*, NEW AM. (Sept. 25, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace [https://perma.cc/SKH7-ZLZU] (archived Jan. 9, 2022); Wang, *supra* note 53, at 453; Gravett, *supra* note 77, at 131.

84. Wang, *supra* note 53, at 455–56.

85. *Id.* at 455.

86. *Id.* at 456; Gravett, *supra* note 77, at 130 (describing a 2017 law that makes social media companies register users with their real names).

87. *See* Wang, *supra* note 53, at 457–58.

88. *See id.*

89. *See id.* at 459–61, 464.

90. *See id.* at 460–61, 464.

Through its "Digital Silk Road," which adopts one of the authors' framings of the internet as the "Electronic Silk Road,"[91] China has sought to advance its digital trade connections with developing countries across the world. This part of China's Belt and Road Initiative promotes collaboration between China and developing countries in critical internet infrastructure projects, e-commerce, and artificial intelligence (AI).[92] By increasing developing African and Eurasian nations' internet access,[93] as well as their dependence on Chinese technology, China acquires soft power while creating new markets for Chinese technology exports and e-commerce.[94] 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.[95] Thus, even as the Chinese government worries about foreign influences via the internet, many other governments worry about the Chinese government exerting its influence via the internet. China looms especially large in the geopolitics that are driving many assertions of digital sovereignty.

C. *The EU: Embracing Digital Sovereignty*

Nowhere have calls for digital sovereignty been more intense than in Europe. As early as 2006, President Jacques Chirac of France called on Europeans to develop an indigenous information search capacity to respond to "the global challenge posed by Google and Yahoo."[96] 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."[97] Among the strategies the government adopted was the promotion of "*le cloud souverain*"—the "sovereign cloud"—through partnerships with cloud computing enterprises to

---

91. ANUPAM CHANDER, THE ELECTRONIC SILK ROAD (2013).

92. *See* Wang, *supra* note 53, at 441.

93. *See id.* at 416–17.

94. *See id.* at 447; Gravett, *supra* note 77, at 131 (international consensus building).

95. *See* Wang, *supra* note 53, at 441–42.

96. CHANDER, *supra* note 91, at 40.

97. Pierre Noro, *Le Cloud Souverain Est De Retour: Généalogie D'une Ambition Emblématique De La Souveraineté Numérique En France*, SCIENCESPO: CHAIRE DIGITAL, GOUVERNANCE ET SOUVERAINETÉ (July 20, 2020), https://www.sciencespo.fr/public/chaire-numerique/2020/07/20/cloud-souverain-genealogie-ambition-emblematique-souverainete-numerique/ [https://perma.cc/U9S9-JHVT] (archived Jan. 9, 2022) (speech by Prime Minister François Fillon on broadband and the digital economy, January 18, 2010).

support domestic employment, among other goals.[98] 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."[99]

EU digital sovereignty has been expressed perhaps most fully through a robust assertion of data protection law. The EU's data protection law covers not only companies based in the EU but also foreign companies that target EU residents and process information about them. This extraterritorial application of law has made the EU into an internet-regulatory superpower.[100]

The German government announced in July 2020 that it would "establish digital sovereignty as a leitmotiv of European digital policy."[101] The European Commission similarly declared its intention to "strengthen its digital sovereignty and set standards, rather than following those of others."[102]

---

98. 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 [https://perma.cc/B5B7-E35P] (archived Jan. 9, 2022). 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).

99. *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://perma.cc/FQE8-YFQQ] (archived Jan. 9, 2022) [hereinafter NEW FACE OF INDUSTRY] (cited in Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 690–91 (2015)). President François Hollande announced the national innovation program on September 12, 2013, with a plan that used the term "sovereignty" no less than a dozen times. *See* Nicholas Vinocur, *Hollande Turns to Robots, Driverless Cars to Revive French Industry*, REUTERS (Sept. 12, 2013), https://www.reuters.com/article/france-industry/hollande-turns-to-robots-driverless-cars-to-revive-french-industry-idUSL5N0H73T020130912 [https://perma.cc/D32G-Z77U] (archived Jan. 9, 2022).

100. ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020) (noting that "the EU remains an influential superpower that shapes the world in its image"); Anupam Chander, Margot E. Kaminski, & William McGeveran, *Catalyzing Privacy*, 105 MINN. L. REV. 1733, 1734 (2021) (explaining that the GDPR's effectuation "positioned the European Union as the world's privacy champion.").

101. TOGETHER FOR EUROPE'S RECOVERY, PROGRAMME FOR GERMANY'S PRESIDENCY OF THE COUNCIL OF THE EU 2020 8 (2020), available at https://www.eu2020.de/blob/2360248/978a43ce17c65efa8f506c2a484c8f2c/pdf-programm-en-data.pdf [https://perma.cc/94WN-XQ4D] (archived Jan. 9, 2022).

102. *A Europe Fit for the Digial* Age, EUR. COMMISSION, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (last visited Jan. 15, 2022) [https://perma.cc/RJ6Z-FKB7] (archived Jan. 15, 2022). The German Presidency of the EU Council declared in 2020, "Europe must bolster its digital sovereignty to effectively respond to future challenges, guarantee livelihoods and ensure the security of its citizens." *See Expanding the EU's Digital Sovereignty*, EU2020, https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828 (last visited Jan. 14, 2022) [https://perma.cc/CW69-GVES] (archived Jan. 9, 2022).

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 from early years when the Russian government embraced the internet as a means to transform the country from reliance on natural resources. In the wake of the Arab Spring, the Russian government began to assert greater control of the internet, recognizing the internet's demonstrated potential to help bring down governments.[103] 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."[104] In 2019, Vladimir Putin signed a "Sovereign Internet" bill into law, gaining broad powers to monitor and control traffic on the Russian internet through hardware and software controls installed in Russian telecommunications infrastructure and even to restrict the global internet in certain cases.[105] Ironically, given prolific Russian interventions in elections abroad, Russian demands for a sovereign internet are driven in part by claims of "information warfare" waged by Western countries against the Russian government.[106] One of the goals of the Runet is to protect the Russian internet from "external negative influences."[107]

Russia employs a common and highly controversial tactic for implementing digital sovereignty: data localization.[108] 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

---

103. *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).

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

105. *See* Ksenia Koroleva, Ulrich Wuermeling, & Tim Wybitul, *RuNet Law Comes into Force: What is Next*, JDSUPRA (Nov. 27, 2019), https://www.jdsupra.com/legalnews/runet-law-comes-into-force-what-is-next-72937/ [https://perma.cc/GAZ8-2UCC] (archived Jan. 9, 2022).

106. Orlova, *supra* note 103, at 231.

107. *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 [https://perma.cc/E6ZQ-FPBX] (archived Jan. 9, 2022).

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

Federation.[109] 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.[110] 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.[111] Roskomnadzor has also threatened to throttle Google's traffic if it refuses to localize data.[112]

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

One nation is more likely to criticize digital sovereignty than to explicitly embrace it: the United States.[113] This is because the United States is in the unique position of being home to many of the world's leading technology firms. This means that during the ordinary course of regulating its companies, the United States exercised digital sovereignty from the start. The US Federal Trade Commission, for

---

109. *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.

110. *See* Adrian Shahbaz, Allie Funk, & Andrea Hackl, *Special Report 2020: User Privacy or Cyber Sovereignty?*, FREEDOM HOUSE, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty (last visited Jan. 14, 2022) [https://perma.cc/R9P9-FHME] (archived Jan. 9, 2022); *Facebook Pays Russia $50K Fine For Not Localizing User Data*, MOSCOW TIMES (Nov. 26, 2020), https://www.themoscowtimes.com/2020/11/26/facebook-pays-russia-50k-fine-for-not-localizing-user-data-a72152 [https://perma.cc/FU37-79KW] (archived Jan. 9, 2022).

111. *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/ [https://perma.cc/R8NF-Z85L] (archived Jan. 14, 2022).

112. *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 [https://perma.cc/DQW5-LJLQ] (archived Jan. 9, 2022).

113. *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/ [https://perma.cc/56DU-AH8J] (archived Jan. 9, 2022).

example, cited GeoCities for privacy failures as early as 1998.[114] There was never a moment when the United States did not exercise digital sovereignty, and thus the United States never had to go out of its way to assert it: it was a natural consequence of the geography of the internet.[115]

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.[116] The United States accused the Russian programmer of selling tools that broke through Adobe's e-book security. Jennifer Granick, a leading digital rights advocate, argued at the time that the United States should not impose its interpretation of copyright law on foreign nations.[117]

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

> Since its inception over two and a half years ago, [US federal] Operation In Our Sites has seized 1,719 domain names of which over 690 have been forfeited, ranging from websites selling allegedly counterfeit luxury goods, sports memorabilia, and pharmaceuticals, to websites that host copyrighted music, movies, TV shows, software, and websites that only link to this content.[118]

But these enforcement actions, Kopel suggests, lack sufficient process and may infringe on free speech concerns.[119]

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

---

114. *FTC, GeoCities Settle on Privacy*, CNET (Aug. 13, 1998), https://www.cnet.com/tech/services-and-software/ftc-geocities-settle-on-privacy/ [https://perma.cc/Y2AG-B78N] (archived Jan. 9, 2022); GeoCities, 127 F.T.C. 94 (1999).

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

116. *See generally* United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002); Robert Lemos, *Russian Crypto Expert Arrested at Def Con*, CNET (Mar. 2, 2002), https://www.cnet.com/news/russian-crypto-expert-arrested-at-def-con/ [https://perma.cc/27EA-6NXY] (archived Jan. 9, 2022). The DMCA criminalizes the sale of tools that break encryption protecting copyrighted works, such as DVDs and e-books.

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

118. 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).

119. *Id.* at 885–93.

Fourth Amendment and statutory protections. But when US prosecutors sought information stored in Ireland on Microsoft servers, Microsoft protested that this was beyond the statutory authority of prosecutors.[120] Congress intervened to amend the law to grant authority to prosecutors to use judicial process to require companies to produce data held abroad.[121]

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 US internet regulation,[122] that era is distinctly over.[123]

At the same time, the US government remains concerned that foreign efforts to assert digital sovereignty can be a guise for old-fashioned protectionism. For example, the US 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."[124]

F. *The Global South: Avoiding Data Colonialism*

Even as access to the internet has grown dramatically,[125] 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).

In 2021, South Africa published a draft "National Data and Cloud Policy" that explicitly seeks to "promote South Africa's data

---

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

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

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

123. *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 [https://perma.cc/BH8L-ST9W] (Jan. 9, 2022); *supra* notes 7–14 and accompanying text (describing antitrust claims against big technology companies).

124. U.S. TRADE REPRESENTATIVE, 2021 NATIONAL TRADE ESTIMATE REPORT ON FOREIGN TRADE BARRIERS 216 (2021).

125. About half of the world's people now have internet access. *Individuals using the Internet*, WORLD BANK, https://data.worldbank.org/indicator/IT.NET.USER.ZS (last visited Jan. 14, 2022) [https://perma.cc/LF98-8XFK] (archived Jan. 9, 2022).

sovereignty."[126] 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."[127] 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."[128] The draft policy also announces, "[d]ata generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled."

In fact, in its recently released "Digital Transformation Strategy for Africa (2020–2030)," the African Union envisions "data sovereignty" as one of its policy priorities.[129] 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."[130] 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.[131] This is part of China's Digital Silk Road effort, tying countries to China through technology.[132]

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.[133] In

---

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

127. *See Data Generated in SA Is the Property of SA, Says New Draft Govt Policy – And Cops Need Access*, BUS. INSIDER SA (Apr. 6, 2021), https://www.businessinsider.co.za/a-draft-national-data-and-cloud-policy-demands-data-sovereignty-for-south-africa-2021-4 [https://perma.cc/954D-3M5X] (archived Jan. 9, 2022).

128. South Africa Dept. of Comm. & Digital Tech., *supra* note 126, at 27.

129. THE DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030), AFRICAN UNION 11 (2020), https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 [https://perma.cc/UZM7-98X3] (archived Jan. 9, 2022).

130. *Id.*; *see* Halefom H. Abraha, *How African Countries Can Benefit From the Emerging Reform Initiatives of Cross-border Access to Electronic Evidence*, CROSS-BORDER DATA FORUM (July 6, 2020), https://www.crossborderdataforum.org/how-african-countries-can-benefit-from-the-emerging-reform-initiatives-of-cross-border-access-to-electronic-evidence/ [https://perma.cc/B5CR-LEY8] (archived Jan. 9, 2022).

131. Dan Swinhoe, *Senegal to Migrate All Government Data and Applications to New Government Data Center*, DATA CTR. DYNAMICS (June 23, 2021), https://www.datacenterdynamics.com/en/news/senegal-to-migrate-all-government-data-and-applications-to-new-government-data-center/ [https://perma.cc/U239-AWE8] (archived Jan. 9, 2022).

132. *See supra* notes 91–95 and accompanying text.

133. *Nigerian Govt Accuses Twitter of Double Standards, Supporting Secessionists*, BUS. STANDARD (June 3, 2021), https://www.business-standard.com/article/international/nigerian-govt-accuses-twitter-of-double-standards-supporting-secessionists-121060300481_1.html [https://perma.cc/2V6Y-GTLV] (archived Jan. 9, 2022). The tweet in question stated: "Many of those misbehaving today

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

Indigenous peoples are also seeking digital sovereignty. Indigenous data sovereignty "deals with the right and ability of tribes to develop their own systems for gathering and using data and to influence the collection of data by external actors."[134] For example, the Māori Data Sovereignty Network seeks to ensure that Māori peoples have sovereignty over the "data produced by Māori or that is about Māori and the environments we [the Māori] have relationships with."[135]

III. HOW DIGITAL SOVEREIGNTY IS DIFFERENT

Digital sovereignty is not merely the assertion of sovereignty online. The last few decades have taught us that the internet changes the nature of sovereignty in a variety of ways. First, because of the global nature of the internet, digital sovereignty almost always has global implications, whether it involves speech regulation, privacy, consumer protection, competition concerns, or law enforcement; thus, digital sovereignty can create significant roadblocks to one of the internet's key virtues—its empowering of global connections. Second, because the digital sphere is intermediated by corporations, the assertion of digital sovereignty typically occurs *vis-à-vis* corporations, not governments. Third, because daily life is increasingly permeated by the internet, digital sovereignty can offer governments surveillance tools that far exceed any history has previously provided. Fourth, because of the dominance of US technology companies globally,

---

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.*

134. 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.").

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

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.[136] 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.[137] The EU's General Data Protection Regulation (GDPR) does not regulate the processing of personal information about a US person in a transaction in the United States, but yet Microsoft and numerous other companies have chosen to apply at least parts of the GDPR to their practices worldwide.[138] Anu Bradford labels this the "Brussels Effect."[139] While David Johnson and David Post famously argued that the global nature of the internet made any sovereign assertion illegitimate,[140] Jack Goldsmith demonstrated that inter-jurisdictional conflicts are not new with the internet and that international law has tools to manage them.[141] Paul Berman goes further to argue that pluralist approaches to governance should be normatively welcome as they better express contemporary conditions.[142]

---

136. *Cf.* Daskal, *supra* note 26, at 185 (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).

137. 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.").

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

139. 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.").

140. *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.").

141. *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

142. Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 490 (2002).

Digital sovereignty increasingly means regulating not only one's citizens alone but also foreigners—typically firms offering services across the world. In order for law to be meaningful in a world of internet globalization, states must regulate foreign entities. It is this necessarily extraterritorial[143] exercise of jurisdiction that increases the difficulty, complexity, and risk of digital sovereignty.

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

B. *Against Corporations*

Where sovereignty has historically been asserted in relation to foreign states, digital sovereignty is equally or perhaps more likely to be asserted against foreign corporations. Foreign corporations are the ones that are dealing directly with their residents—collecting data, offering services, and moderating speech. Jennifer Daskal observes that much of transnational internet governance "is largely being mediated by the private parties that hold and manage our data."[144] She writes, "It is these companies that increasingly determine whose rules govern and, in key ways, how they are interpreted and applied," she writes.[145] Writing about digital sovereignty, Lucien Floridi observes, "The most visible clash is between companies and states."[146]

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."[147] Much of the enforcement activity under the GDPR is, accordingly, targeted at corporations. Much as some US residents worry about the exploitation of their data by US companies,

---

143. 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.

144. Daskal, *supra* note 26, at 185.

145. *Id.*

146. *See* Floridi, *supra* note 26, at 371.

147. *See* EUR. PARLIAMENTARY RES. SERV., DIGITAL SOVEREIGNTY FOR EUROPE 1 (2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf. [https://perma.cc/P7GH-D5C4] (archived Jan. 9, 2022).

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.[148]

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."[149] 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."[150]

In *Seeing Like a State*, historian James C. Scott argues that increases in what he calls "legibility" (the ability of the state to better understand its population) were a critical part of large governmental projects.[151] 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, which Julie Cohen observes,[152] can be exploited by the state as well.

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."[153] 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.[154] We should be mindful that digital regulators, whether well-intentioned or

---

148. *Mukesh Ambani Says 'Data Colonisation' as Bad as Physical Dolonisation*, ECON. TIMES (Dec. 19, 2018), https://economictimes.indiatimes.com/news/company/corporate-trends/mukesh-ambani-says-data-colonisation-as-bad-as-physical-colonisation/articleshow/67164810.cms?utm_source%3Dtwitter_web%26utm_medium%3Dsocial%26utm_campaign%3Dsocialsharebuttons [https://perma.cc/9WYG-2RVQ] (archived Jan. 9 2022).

149. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1936 (2013).

150. 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).

151. *See generally* JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED (1998).

152. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 38 (2019).

153. SCOTT, *supra* note 151, at 342.

154. *Id.* at 346.

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."[155] Günther Oettinger, then a member of the European Commission for Budget and Human Resources, explained that "[t]he digital single market can be a win-win" for both European and Silicon Valley firms.[156] Andrus Ansip, the European Commissioner for Digital Single Market from 2014 to 2019, similarly suggested, "[t]he digital single market will provide opportunities for trade, investment, innovation not only for Europe, but globally—also, for the United States."[157] Fredrik Persson, chairman of the Confederation of Swedish Enterprise cautioned that European efforts towards digital sovereignty "should not create a European fortress that pulls up the drawbridge to the outside world."[158] 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."[159] Many European

---

155. Hamza Shaban, *European Union Unveils Digital Single Market Plan*, BUZZFEED NEWS (May 6, 2015), https://www.buzzfeednews.com/article/hamzashaban/european-union-unveils-digital-single-market-plan [https://perma.cc/35CX-V4ZJ] (archived Jan. 14 2022); *see* David O'Sullivan, *Stop the Hysteria: Of Course, Europe Wants an Open Internet*, WIRED (Apr. 30 2015), https://www.wired.com/2015/04/eu-ambassador-on-open-internet/ [https://perma.cc/CX98-AESM] (archived Jan. 9 2022).

156. Hamza Shaban, *EU Digital Commission to Silicon Valley: Relax*, BUZZFEED NEWS (Sept. 25, 2015), https://www.buzzfeednews.com/article/hamzashaban/eu-digital-commissioner-to-silicon-valley-relax [https://perma.cc/5XT6-CR2N] (archived Jan. 9 2022).

157. Hamza Shaban, *Digital Single Market Isn't Anti-American, Says EU Commissioner*, BUZZFEED NEWS (May 28, 2015), https://www.buzzfeednews.com/article/hamzashaban/digital-single-market-isnt-anti-american-says-eu-commissione [https://perma.cc/AQ87-38BR] (archived Jan. 9 2022).

158. Christakis, *supra* note 26, at 58.

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

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

Other voices within the EU, however, portray issues of digital sovereignty as a zero-sum geopolitical struggle. In 2019, French President Emmanuel Macron declared, "[t]he battle we're fighting is one of sovereignty." He continued, "[i]f we don't build our own champions in all new areas—digital, artificial intelligence—our choices . . . will be dictated by others."[160] 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."[161] Commissioner Thierry Breton declares that "European data will be used for European companies in priority, for us to create value in Europe."[162]

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 US roads, Americans no longer control their streets. As long as the cars are regulated by local law, the fact that they might be built abroad should not undermine sovereignty.

Some see a zero-sum game with respect to the internet with winners and losers. In 2020, Thierry Breton, the European Union's Commissioner for Internal Market, expressed confidence that EU companies would beat their American counterparts: "The winners of today will not be the winners of tomorrow."[163] At times, however, the European approach to digital sovereignty seems to be focused on replacing US enterprises with European ones, a classic protectionist strategy. Commissioner Breton seeks to ensure that "European data

---

faster-european-digital-sovereignty [https://perma.cc/W4G5-ASKF] (archived Jan. 9 2022).

160. 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/ [https://perma.cc/G887-BUY3] (archived Jan. 9 2022). 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.

161. DIGITAL SOVEREIGNTY FOR EUROPE, *supra* note 147.

162. FRANCES BURWELL & KENNETH PROPP, THE EUROPEAN UNION AND THE SEARCH FOR DIGITAL SOVEREIGNTY: BUILDING "FORTRESS EUROPE" OR PREPARING FOR A NEW WORLD? 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 [https://perma.cc/SGH4-P5YS] (archived Jan. 9 2022).

163. Foo Yun Chee, *This is the EU's plan to compete with Silicon Valley*, WORLD ECON. F. (Feb. 20, 2020), https://www.weforum.org/agenda/2020/02/eu-data-market-technology-silicon-valley [https://perma.cc/E8VL-Y5GM] (archived Jan. 9 2022).

will be used for European companies in priority, for us to create value in Europe."[164]

Even while seeking to rein in the power of US tech titans, some in the EU seem to covet their own. In June 2021, "French President Emmanuel Macron announced the objective of having '10 companies worth €100 billion by 2030' in Europe . . . after he received . . . recommendations to encourage the emergence of digital giants in Europe."[165] Some in the EU wish to create their own "European digital champions."[166] 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.[167]

IV. 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. This Part examines a number of ways in which that power can lend itself to abuse. Even well-intentioned law—in the examples discussed here that are designed to protect against abusive speech or to protect privacy or national security—can be prone to abuse. This Part offers examples of this possibility, 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 acerbly noted that the "most common use of the word 'sovereignty' may be in sovereign immunity--immunity from law, immunity from scrutiny, immunity from justice."[168]

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

---

164. BURWELL & PROPP, *supra* note 162.

165. *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/ [https://perma.cc/84N3-JCTY] (archived Jan. 9 2022).

166. *See* Christakis, *supra* note 26, at 89.

167. Georgia Wells, Jeff Horwitz, & Aruna Viswanatha, *Facebook CEO Mark Zuckerberg Stoked Washington's Fears About TikTok*, WALL ST. J. (Aug. 23, 2020), https://www.wsj.com/articles/facebook-ceo-mark-zuckerberg-stoked-washingtons-fears-about-tiktok-11598223133#:~:text=Zuckerberg%20told%20Georgetown%20students%20that,American%20values%20and%20technological%20supremacy [https://perma.cc/L6EK-YJ2N] (archived Jan. 9 2022).

168. *See* Henkin, *supra* note 20, at 13.

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,[169] that seems distinctly more dangerous[170] than European Union obligations for maintaining a local representative.[171] 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 by government orders.[172] The intermediary rules requiring local grievance officers seem to have been instituted by Prime Minister Narendra Modi's government following its displeasure with Twitter.[173]

A. *Speech*

1. 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

---

169. *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/ [https://perma.cc/GT73-H42J] (archived Jan. 9 2022).

170. *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 [https://perma.cc/K79S-U42Q] (archived Jan. 9 2022).

171. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 27, 2016 O.J. (L 119), 1 (requiring local representative of foreign data controllers or processors that lack a local establishment).

172. *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://perma.cc/UNQ9-9UP6] (archived Jan. 9 2022). 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 24×7 coordination with law enforcement agencies and officers," and a grievance officer who will be responsible for all functions mentioned under the grievance redressal mechanism. *See also Modi Govt Announces New Rules to Tighten Oversight Over Social Media, Digital Media Platforms, Streaming Services*, 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 [https://perma.cc/TDB2-LNMR] (archived Jan. 9 2022).

173. Aditya Kalra & Sankalp Phartiyal, *India Plans New Social Media Controls After Twitter Face-Off*, REUTERS (Feb. 24, 2021 10:19 AM), https://www.reuters.com/article/us-india-tech-regulation/india-plans-new-social-media-controls-after-twitter-face-off-idUSKBN2AO201 [https://perma.cc/F532-TEVZ] (archived Jan. 14, 2022).

regulators," Diana Lee writes.[174] 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.[175] NetzDG specifies twenty-two offenses that require such rapid deletion, including libel, defamation, sedition, and calls for violence. As Lee notes, "[i]n close cases, social media companies will likely err on the side of caution in order to avoid penalties under the NetzDG."[176] Many worry about the possibility of over-blocking content, given the penalties for non-compliance with the takedown obligation.[177]

By requiring incredibly rapid takedowns, such laws "virtually require the use of upload filters," as Hannah Bloch-Wehba argues.[178] 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."[179] 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."[180] 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."[181] Facebook's "X-check" internal process, which exempts some high-profile users, including politicians, from the automated application of its rules, further demonstrates this dynamic.[182]

---

174. Diana Lee, *Germany's NetzDG and the Threat to Online Free Speech*, MEDIA FREEDOM & INFO. ACCESS CLINIC (Oct. 10, 2017), https://law.yale.edu/mfia/case-disclosed/germanys-netzdg-and-threat-online-free-speech [https://perma.cc/97YV-HAFN] (archived Jan. 14, 2022).

175. *Id.* (quoting James Q. Whitman, *Enforcing Civility and Respect: Three Societies*, 109 YALE L.J. 1279, 1297 (2000)).

176. *Id.*

177. Amelie Heldt, *Reading Between the Lines and the Numbers: An Analysis of the First NetzDG Reports*, 8(2) INTERNET POL'Y REV. 1, 5 (2019).

178. 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." *See also id.* at 70.

179. *Id.* at 46.

180. *Id.*

181. Annemarie Bridy, *Moderation's Excess*, JOTWELL (Mar. 27, 2020), https://cyber.jotwell.com/moderations-excess/ [https://perma.cc/PW5G-K57F] (archived Jan. 9, 2022).

182. Jeff Horwitz, *Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt*, WALL. ST. J., (Sept. 13, 2021), https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353 (last visited Jan. 9, 2022) [https://perma.cc/68ML-LQN3] (archived Jan. 9 2022).

2. *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"?[183] 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[184] 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 circumstances indicating illegal activity."[185] Recital 47 of the E-Commerce Directive, however, permits monitoring obligations in a specific case—such as the one in Glawischnig-Piesczek.[186] The CJEU went further to conclude that the Austrian court could not only order the deletion of the particular post, but also prevent any post with content that is "equivalent" across Facebook sites "worldwide."[187]

The demand to remove posts "having equivalent meaning" across Facebook worldwide seems to require automated systems that are likely to produce significant errors.[188] 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

183. 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).

184. 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.

185. *Id.* at art. 15.

186. Felipe Romero Moreno, *'Upload Filters' and Human Rights: Implementing Article 17 of the Directive on Copyright in the Digital Single Market*, 34 INT'L REV. L., COMPUTERS & TECH., 153, 154 (2020).

187. Case C-18/18, Eva Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821, ¶ 53 (Oct. 3, 2019).

188. *See* NATASHA DUARTE, EMMA LLANSÓ, & ANNA LOUP, MIXED MESSAGES? THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS (2017); *see also* Emma Llansó, *No Amount of "AI" in Content Moderation Will Solve Filtering's Prior-Restraint Problem*, 7 BIG DATA & SOC'Y 1 (2020).

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 Facebook was governed by either Irish law (because of its European headquarters) or US 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.[189]

B. *Privacy*

1. Justice Reform Act (France)

In 2016, lawyer and machine-learning expert Michaël Benesty analyzed French asylum decisions by judges, revealing that some judges rejected almost all asylum requests while others accepted most.[190] 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.[191] The 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."[192] Such a law makes it more difficult to scrutinize the judicial process and to identify judges that might be hostile to particular claims.

---

189. *See* CHANDER, *supra* note 91, at 34 (2013) (arguing that "public policy objectives cannot easily be evaded through a simple jurisdictional sleight of hand or keystroke").

190. Malcolm Langford & Mikael Rask Madsen, *France Criminalises Research on Judges*, VERFASSUNGSBLOG (June 22, 2019), https://verfassungsblog.de/france-criminalises-research-on-judges/ [https://perma.cc/25VH-WYJF] (archived Jan. 9 2022).

191. *See France Bans Judge Analytics, 5 Years in Prison for Rule Breakers*, ARTIFICIAL LAW. (June 4, 2019), https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/ [https://perma.cc/2BWD-8SGQ] (archived Jan. 9 2022). 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 scrutinized too closely either." *See also id.*

192. Jason Tashea, *France Bans Publishing of Judicial Analytics and Prompts Criminal Penalty*, ABA J. (June 7, 2019, 12:51 PM), https://www.abajournal.com/news/article/france-bans-and-creates-criminal-penalty-for-judicial-analytics (quoting translation by Rebecca Loescher) [https://perma.cc/2JRP-GDYD] (archived Jan. 9 2022) (original text available at https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038261761?r=LEGAIp0IBR [https://perma.cc/BE5F-5QP6] (archived Jan. 9 2022)).

2. Data Protection/Didi (China)

On June 30, 2021, Didi, the ride-hailing firm based in Beijing, went public on the New York Stock Exchange.[193] 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.[194] The cybersecurity review was aimed at "preventing national data security risks, maintaining national security and safeguarding public interests."[195] CAC ordered the app removal because it found that the app was "illegally collecting and using personal information."[196] 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."[197] 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."[198] Zuo Xiaodong, the vice president of the China Information Security Research Institute, similarly stated, "[i]n 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."[199]

The concerns are similar, at least on one level, to those expressed by the CJEU 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 US law did not sufficiently protect the data of foreigners from American governmental surveillance.[200] In that

193. Kate Conger & Raymond Zhong, *Didi, the Chinese Ride-Hailing Giant, Makes Its Debut on Wall Street*, N.Y. TIMES (June 30, 2021), https://www.nytimes.com/2021/06/30/technology/didi-wall-street-initial-public-offering.html [https://perma.cc/Z9PX-FR7V] (archived Jan. 9 2022).

194. *See* 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/ [https://perma.cc/MWD8-SBEJ] (archived Jan. 9, 2022).

195. *Id.*

196. *See id.*

197. 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 [https://perma.cc/62CA-3VDE] (archived Jan. 9, 2022).

198. *Id.*

199. *Id.*

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

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 US 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*

1. 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."[201] 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,[202] followed by another order requiring ByteDance, the Beijing-based owner of TikTok, to divest its US TikTok subsidiary following a national security review by the Committee on Foreign Investment in the United States (CFIUS).[203] Through TikTok, the President argued, the Chinese government could secretly compile compromising data about Americans, enabling blackmail.[204] The Trump administration

---

201. 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 [https://perma.cc/K6Z7-SX9N] (archived Jan. 9, 2022).

202. 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 property, subject to the jurisdiction of the United States" would be prohibited from transacting with ByteDance Ltd., the Chinese owner of TikTok, 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 . . .") (emphasis added); Proclamation No. 10,061, 84 Fed. Reg. 51,295 (Sept. 27, 2019) (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://2017-2021.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect.html [https://perma.cc/LP5Q-8FS2] (archived Jan. 9, 2022).

203. *See* 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.).

204. *See* TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 77 (D.D.C. 2020).

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.[205] 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.[206]

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. He declared that if his opponent won the election, "You're going to have to learn to speak Chinese."207 But when federal courts saw the government's secret evidence against TikTok, they sided with TikTok, preliminarily enjoining the TikTok and WeChat bans.[208] 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.[209] In a second case, Judge Wendy Beetlestone declared the government's concerns "hypothetical."[210] 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.[211] Trump borrowed even more of the authoritarian

---

205. *See* 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 [https://perma.cc/6L7L-8RPH] (archived Jan. 9, 2022).

206. Authors' independent search on TikTok app on May 10, 2021.

207. Kevin Liptak, *Trump Says Americans Will Have to Learn Chinese if Biden Wins but Offers Little Condemnation of Beijing,* CNN (Aug. 11, 2020, 1:58 PM), https://www.cnn.com/2020/08/11/politics/trump-china-biden-learn-chinese/index.html [https://perma.cc/KD3W-LM6Y] (archived Jan. 9, 2022).

208. *See* 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.").

209. *See* 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.").

210. Marland v. Trump, 498 F. Supp. 3d 624, 642 (E.D. Pa. 2020).

211. *See* Stuart Emmrich, *Is Sarah Cooper the Reason Donald Trump Wants to Ban TikTok?*, VOGUE (Aug. 1, 2020), https://www.vogue.com/article/is-sarah-cooper-the-reason-donald-trump-wants-to-ban-tik-tok [https://perma.cc/B7U8-UD5P] (archived Jan. 9, 2022). Under this theory, the WeChat ban would be merely collateral damage, as

internet playbook than might be obvious: like authoritarians everywhere, he sought to silence his critics. TikTok had already proven a thorn in his side, with comedian Sarah Cooper using the platform to lampoon him, and teens coordinating via TikTok to claim tickets to his rally so as to leave the arena mostly empty.[212] TikTok, after all, was the one massive social media platform in the United States 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.[213]

In 2021, a new president would revoke the TikTok and WeChat bans, ordering instead a broad review of access to US persons' sensitive data by foreign adversaries.[214] President Biden 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."[215] 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

---

it would be odd to target TikTok without also banning this other popular Chinese-owned app.

212. Chander, *supra* note 21, at 24.

213. *See* Adam Conner, *Trump's Facebook Account Should Never Be Reinstated Because We Know What He'd Use It For*, NBC (May 3, 2021, 7:07 PM), https://www.nbcnews.com/think/opinion/trump-s-facebook-account-should-never-be-reinstated-because-we-ncna1266182 [https://perma.cc/3ZDU-EW3B] (archived Jan. 9, 2022) (former President Trump maintained roughly 32 million Facebook followers); Trump Tweets Can't Be Brought Back To Life on Twitter, BBC (Apr. 8, 2021), https://www.bbc.com/news/technology-56675272 [https://perma.cc/DDL2-JCG5] (archived Jan. 9, 2022) (Former President Trump maintained roughly 90 million Twitter followers); Donald J. Trump, YOUTUBE, https://www.youtube.com/channel/UCAql2DyGU2un1Ei2nMYsqOA (last visited Jan. 9, 2022) [https://perma.cc/23RF-YWX7] (archived Jan. 9, 2022) (former President Trump maintained roughly 2.7 million subscribers on his frozen YouTube channel).

214. *See* Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021) [hereinafter Protecting Americans' Sensitive Data]; *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 [https://perma.cc/HM23-C5AR] (archived Jan. 9, 2022). The Biden Administration has not yet withdrawn the CFIUS executive order requiring divestiture, but does not seem to be enforcing that order.

215. Protecting Americans' Sensitive Data, *supra* note 214.

the otherwise broad emergency economic powers that Congress granted to the president.[216]

2. NSO Spyware for Hire (Israel)

In July 2021, Amnesty International revealed that some fifty thousand individuals in more than forty-five countries—including fourteen heads of state[217] and numerous journalists—were the target of phone hacking using software sold by the NSO Group.[218] 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."[219] In 2021, the iPhones of U.S. Embassy employees working in Uganda were reportedly hacked using spyware developed by the NSO Group.[220]

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.[221] Its IPO prospectus warns investors

---

216. *See* 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 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).

217. *See* Peter Beaumont & Philip Oltermann, *Israel to Examine Whether Spyware Export Rules Should be Tightened*, GUARDIAN (July 22, 2021, 11:45 AM), https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus [https://perma.cc/366P-2TMQ] (archived Jan. 9, 2022).

218. Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, & Michael Safi, *Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon*, GUARDIAN (July 18, 2021, 12:00 PM), https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus [https://perma.cc/UUU2-TFJU] (archived Jan. 9, 2022).

219. *Id.*

220. *See* Christopher Bing & Joseph Menn, *U.S. State Department Phones Hacked With Israeli Company Spyware*, ROUTERS (Dec 4, 2021), https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/.

221. *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

that its "solutions may be used by customers in a way that is, or that is perceived to be, incompatible with human rights."[222] Another Israeli "hacking-for-hire" firm, Candiru, has helped government clients spy on "politicians, human rights activists, journalists, academics, embassy workers and political dissidents," at least according to Microsoft.[223] The Israeli company Verint Systems reportedly sold spying tools to Azerbaijan that were used to identify its citizens' sexual orientations through Facebook and sold to Indonesia to collect personal information about LGBT rights activists.[224]

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 United Arab Emirates.[225] The US 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.[226] 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.[227]

[https://perma.cc/5TW6-SDSL] (archived Jan. 9, 2022); *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-idUSL8N2OO5IP [https://perma.cc/73MU-W7YK](archived Jan. 9, 2022).

222. Cellebrite DI Ltd., Registration Statement, Registration No. 333-256177 (June 29, 2021), at 27.

223. Cristin Goodwin, *Fighting Cyberweapons Built by Private Businesses*, MICROSOFT (July 15, 2021), https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/ [https://perma.cc/W25F-JP5X] (archived Jan. 9, 2022); *see* Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, & Ron Deibert, *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/ [https://perma.cc/ULC9-9HBX] (archived Jan. 9, 2022).

224. *See* Jason Murdock, *Israeli Companies Sold Surveillance Tech and Knowledge Used for Persecuting Dissidents, Journalists, LGBT People*, NEWSWEEK (Oct. 19, 2018), https://www.newsweek.com/Israeli-companies-sell-surveillance-tech-and-knowledge-used-persecuting-1178084 [https://perma.cc/RV4E-VSTV] (archived Jan. 9, 2022).

225. *See* Alex Hern, *Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim*, GUARDIAN (July 6, 2015, 7:46 PM), https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim [https://perma.cc/Q3PA-YJ3D] (archived Jan. 9, 2022).

226. *See* Ryan Gallagher, *U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet*, BLOOMBERG (Sept. 11, 2020), https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers (subscription required).

227. *See* AMNESTY INT'L, OPERATING FROM THE SHADOWS: INSIDE NSO GROUP'S CORPORATE STRUCTURE 7 (2021).

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.[228] But why use Chinese surveillance technology when one can buy Western technology that will get the job done?[229] And this argument seems to forget that it was Western companies that helped build China's Great Firewall in the first instance.[230]

Israeli law requires exports of such spyware to be approved by its Defense Department, and NSO claims to have received the necessary permits.[231] 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 noted 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."[232] 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

---

228. *See, e.g.*, U.S. DEP'T OF STATE, 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 & CHRIS MESEROLE, EXPORTING DIGITAL AUTHORITARIANISM 5–6 (2019), https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf [https://perma.cc/KG4Z-XACH] (archived Jan. 9, 2022).

229. *Cf.* Maya Wang, *China's Techno-Authoritarianism Has Gone Global*, FOREIGN AFFS. (Apr. 8, 2021), https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global [https://perma.cc/8NGR-ESQP] (archived Jan. 15, 2022) (observing that while countries from 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.").

230. 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 *(IHT)* used to censor web content, and 'firm's engineers have helped set it to spot 'subversive' key-words in messages.'" Robert McMahon & Isabella Bennett, *U.S. Internet Providers and the 'Great Firewall of China'*, COUNCIL FOREIGN RELS. (Feb. 23, 2011, 7:00 AM), https://www.cfr.org/backgrounder/us-internet-providers-and-great-firewall-china [https://perma.cc/2L7B-G8T7] (archived Jan. 9, 2022).

231. *See* Defense Export Control Law 5766-2007 (Isr.).

232. *See* Anonymous, *I Worked at Israeli Phone Hacking Firm Cellebrite. They Lied to Us*, HAARETZ (July 27, 2021), https://www.haaretz.com/israel-news/i-worked-at-israeli-phone-hacking-firm-cellebrite-they-lied-to-us-1.10041753 [https://perma.cc/AZ3H-5AVT] (archived Jan. 9, 2022).

of jointly pressuring foreign governments to stop permitting their companies to sell such services in the global markets.[233]

V. 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.[234] Yahoo!'s lawyers responded that to apply French law to a site based in the United States more closely resembled French imperialism.[235] The French court carefully tailored its order to only require Yahoo! to desist from providing the prohibited materials within France.[236] 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.[237] (The French themselves have gone on occasion further to demand global takedowns of information—a radical and alarming assertion of jurisdiction.[238])

A quarter of a 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, there are increasing efforts by the countries of the world to gain control over the internet. This is understandable. As Andrew Woods observed, "states remain the single greatest source of legitimate rules for different peoples with varied community values and experiences on a diverse planet."[239] States make the law and enforce it, hopefully for our protection. There is at present no international substitute for such protection. 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 our work, school, and private lives—but scary because regulation of the internet

---

233. For a related argument for a national statute backed by an international treaty to regulate information services that operate in repressive jurisdictions, *see* Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 36–44 (2011).

234. *See* Greg Wrenn, *Yahoo! V. LICRA*, 24 COMM. LAW. 5, 5–6 (2006).

235. *See id.* at 6.

236. *See id.* at 6–7.

237. 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), *rev'd and remanded*, 433 F.3d 1199 (9th Cir. 2006).

238. Kevin Benish, *Whose Law Governs Your Data?: Takedown Orders and "Territoriality" in Comparative Perspective*, 55 WILLAMETTE L. REV. 599, 615–19 (2019) (describing French application of the right to be forgotten worldwide); *see generally* Jennifer Daskal, *Speech Beyond Borders*, 105 VA. L. REV. 1605 (2019).

239. Woods, *supra* note 16, at 369.

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 themselves.