BOOK REVIEW

The Geopolitics of Digital Regulation

Aziz Z. Huq†

Contemporary regulation of new digital technologies by nation-states unfolds under a darkening shadow of geopolitical competition. The United States government operates simultaneously in a domestic political environment dominated by oligopolistic firms competing to expand, and in an international political environment wherein it competes against other sovereign nations by cultivating and deploying digital technological capacities for geostrategic economic and military ends. Thanks to the ensuing burst of crosscutting pressures, both national and supranational regulation can take on surprisingly reticulated, even baroque or perverse, forms.

Three recent monographs offer illuminating and complementary maps of these geopolitical conflicts and the national responses to digital technologies unfolding under their aegis. One proposes an ambitious, synoptic account of how geopolitical dynamics unfold: it is, impressively, the only genuinely all-embracing account of the field on offer at the moment—albeit one with distinctive analytic and predictive asymptotes. The other two books develop more narrowly drawn descriptive accounts that focus on specific regulatory dynamics. These depictions are still useful, but more limited in scope than a synoptic view.

Folding together insights from all three books, however, opens up pathways toward a new, more perspicacious understanding of geopolitical dynamics, and hence a vantage point on the most likely future of digital regulation. This perspective, informed by all three books under consideration here, suggests grounds for skepticism about the emergence of a deep regulatory equilibrium, celebrated by many, in expectation centered on the emerging slate of European laws. While regulatory regimes may reach for common solutions, the policy convergence reflects no meaningful European hegemony. Further, the area of overlap will be strictly limited to less important questions by growing bipolar geostrategic conflict between the United States and China. Ambitions for global regulatory convergence when it comes to new digital technology, therefore, should be modest.

† Frank and Bernice J. Greenberg Professor of Law, The University of Chicago Law School, supported by the Frank J. Cicero fund. Thanks to Uven Chong for research assistance. Anu Bradford offered gracious, insightful, and generous comments on a draft that strikes to be fair, if critical, of her work. For her careful engagement, I am respectfully and deeply grateful. Editors of the *University of Chicago Law Review*, including Helen Zhao, Daniella Apodaca, and Nathan Hensley, did excellent work on the text.

INTRODUCTION

The contemporary regulation of digital technologies by nation-states unfolds under a darkening sky bright with the fearful harbingers of geopolitical competition. Instilling fear or envy in equal measures, foreign actors shape both federal and state responses to the new digital tools for communication, data analysis, prediction, and preference manipulation. The results are often unexpected, perhaps counterproductive, flares of regulatory temper.

Consider three examples from the last couple of years:

- In April 2024, Congress singled out one of the most popular social media apps among young people in the United States, TikTok, and mandated that its Chinese owner ByteDance divest within 270 days, or else face a permanent ban on its product.[1] Ostensibly, Congress's justification for picking out TikTok from a bevy of other apps

[1] Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024) [hereinafter PAFACA]; Sapna Maheshwari & David McCabe, *Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part*, N.Y. TIMES (Apr. 23, 2024), https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html.

scraping and selling personal data had been its foreign (Chinese) ownership in particular, which was seen as a source of security risks absent from U.S.-owned or multinational platforms.[2]

- A month after Congress moved against TikTok, Colorado enacted one of the nation's first comprehensive legislative packages to regulate artificial intelligence (AI).[3] The state, however, eschewed the approach suggested by the then-leading federal initiatives. An earlier, much-trumpeted White House measure called the *Blueprint for an AI Bill of Rights*, for instance, proposed to address new technology by isolating specific rights that must be respected.[4] In contrast, Colorado's law does not work by picking out rights, but rather is "[s]imilar" in regulatory style to the 2024 European Union (EU) AI Act[5]: the latter taxonomizes different kinds of AI risk in terms of the magnitude of harm emanating from each one, and then extends distinct ex ante mandates to each.[6]
- Concurrent to these efforts to regulate private parties' primary conduct, a more subterranean thread of geopolitical conflict unspools through an escalating spiral of tit-for-tat

---

[2] Concerns about Chinese influence motivated the initial efforts to ban TikTok. *See* Mark Jia, *American Law in the New Global Conflict*, 99 N.Y.U. L. REV. 636, 671 (2024) [hereinafter Jia, *American Law*]. The nature of the threat from China played a pivotal role in litigation over earlier iterations of the divestiture mandate. *See* TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 85 (D.D.C. 2020) (finding that "the government has provided ample evidence that China presents a significant national security threat"). In December 2024, the U.S. Court of Appeals for the District of Columbia Circuit issued a decision upholding the measure, whereupon the Supreme Court granted certiorari. *See generally TikTok Inc. v. Garland*, 122 F.4th 930 (D.C. Cir. 2024), *cert. granted*, 2024 WL 5148087 (Dec. 18, 2024), *and cert. granted sub nom.* Firebaugh v. Garland, 2024 WL 5148088 (Dec. 18, 2024). On January 17, 2025, as this writing was in the final stages of production, the Supreme Court unanimously upheld the measure in a decision that is striking for its languorous indifference to the (hardly implausible) prospect that the federal government could deploy concerns about the security of data on any social media platform to exert exorbitant control over its content. *See generally TikTok v. Garland*, 145 S. Ct. 57 (2025) (per curiam).

[3] *See* COLO. REV. STAT. §§ 6-1-1701 to -1707 (2024).

[4] *Blueprint for an AI Bill of Rights*, THE WHITE HOUSE, https://perma.cc/N88B-7CLE.

[5] Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L 1689).

[6] Marian A. Waldman Agarwal & Marijn Storm, *Navigating New Frontiers: Colorado's Groundbreaking AI Consumer Protection Law*, MORRISON & FOERSTER (May 31, 2024), https://perma.cc/7Q5Q-HH56 (noting parallels between regulation of AI by Colorado and the European Union).

> trade restrictions. These are lobbed mostly by China and the United States against the transnational flow of raw materials and finished semiconductors necessary for advanced digital tools.[7] Likewise, a complex skein of U.S. statutes and regulations, enforced by the Commerce, Treasury, and Homeland Security Departments, and independent agencies, shape cross-border data flows.[8] All such rules are subject to sudden, seemingly inexplicable involutions. In October 2023, for example, the U.S. Trade Representative Katherine Tai suddenly "dropped" long-standing U.S. resistance to data localization measures in trade negotiations—presumably because the United States increasingly sees the value of hoarding its own data reservoirs.[9]

These examples illustrate some of the many ways in which the United States "is operating simultaneously in a domestic political environment dominated by firms competing to expand and monetize [technology]" and "simultaneously in an international environment in which it is competing with other sovereign nations that are cultivating and deploying the same technological capacities for geostrategic ends."[10]

As a result of these crosscutting pressures from international interest groups and external sovereigns or firms, domestic regulation can take on surprisingly reticulated, even baroque, forms. In the case of TikTok, such pressures induced lawmakers to carve

---

[7] *Compare* Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification; Updates to the Controls to Add Macau, 88 Fed. Reg. 2821 (Oct. 7, 2023) (to be codified at 15 C.F.R pts. 734, 736, 740, 742, 744, 762, 772, and 774), *with* Alan Rappeport, Keith Bradsher & Ana Swanson, *Yellen's China Visit Aims to Ease Tensions Amid Deep Divisions*, N.Y. TIMES (July 4, 2023), https://www.nytimes.com/2023/07/04/business/economy/janet-yellen-china.html. China also filed a complaint with the World Trade Organization. Request for Consultations by China, *United States—Measures on Certain Semiconductor and Other Products, and Related Services and Technologies*, WTO Doc. WT/DS615/1 (Dec. 15, 2022).

[8] AYNNE KOKAS, TRAFFICKING DATA: HOW CHINA IS WINNING THE BATTLE FOR DIGITAL SOVEREIGNTY 28–33 (2023) (summarizing this regulatory framework).

[9] David Lawder, *US Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation*, REUTERS (Oct. 25, 2023), https://www.reuters.com/world/us/us-drops-digital-trade-demands-wto-allow-room-stronger-tech-regulation-2023-10-25/.

[10] Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer*, 76 N.Y.U. ANN. SURV. AM. L. 317, 320 (2021).

out and target specific foreign firms.[11] Or, as the recent U.S. volte-face on data localization illustrates, it can lead to broad-brush policymaking aimed to protect against almost all foreign interests.

Adding to the situation's complexity, nation-states are not the only source of new rules. Internationally, path-marking treaties, trade deals, and shared technical standards can also emerge through the joint action of bodies such as the European Union,[12] the Council of Europe,[13] or the Shanghai Cooperation Organization.[14] As a result, the overall legal regimes for digital technologies contain both domestic rules (often crafted with an eye to extraterritorial effects) and also transnational regimes (shaped in turn by the domestic agendas of participating nations). Both kinds of regulation must be layered over the existing private governance regimes worked up by private firms, many exercising monopoly power, in their internal operating procedures or their terms of service.

The tapestry of law that results from these overlapping regulatory initiatives is one eddied by discontinuity, conflict, and instability. Disciplining such complexities requires, at a minimum, a careful empirical inquiry into various kinds of geopolitical competition. This is no simple matter. The technical difficulty of digital tools and the many ways in which their uses can be shaped by law impose formidable barriers to any effort at clear accounting. Even with those details in hand, it is still necessary to abstract away from the rich doctrinal detail of the world, and to refine a parsimonious model that can serve as a guide to the unforgiving new landscape. This guards against the risk of being lost in detail, and so unable to see the basic contours of the regulatory landscape.

---

11 To be sure, federal law contains other prohibitions on data transfers to foreign entities. *See, e.g.*, 15 U.S.C. § 9991 (making it "unlawful for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual" to an entity controlled by a "foreign adversary country").

12 *See, e.g.*, *Artificial Intelligence Act: MEPs Adopt Landmark Law*, EUR. PARLIAMENT (Mar. 13, 2024), https://perma.cc/D6S7-6RLW.

13 *See, e.g.*, *Text of First Legally Binding Global Instrument to Address Risks Posed by Artificial Intelligence Finalised by the Council of Europe*, DELEGATION OF EUR. UNION TO COUNCIL OF EUR. (Apr. 2, 2024), https://perma.cc/4RNA-U8H3.

14 *See* Tate Ryan-Mosley, *The World Is Moving Closer to a New Cold War Fought with Authoritarian Tech*, MIT TECH REV. (Sept. 22, 2022), https://perma.cc/2YTY-ZDYK (arguing that the Shanghai Cooperation Organization has been a key vector for disseminating tools of "digital authoritarianism").

Such a useful model of digital regulation's geopolitical context must have several features: It will acutely pick out the central incentives of nation-states. It will account for the relative efficacy or disutility of different regulatory tools. It will have ample play in the joints for the interplay between domestic politics and international strategy.[15] And it will strike an appropriate balance between an accent on the stabilizing force of institutions on the one hand, and an emphasis on the disruptive effect of national ideologies or technical breakthroughs on the other.[16]

Three recent monographs take important steps forward in this large project. Each offers illuminating, if only partially complementary, analyses of recent geopolitical conflicts over new digital technologies. One proposes an ambitious, synoptic account of how geopolitical dynamics unfold. Impressively, it is the only genuinely all-embracing *coup d'oeil* on offer at the moment. As such, it merits the lion's share of our attention—scrutiny that reveals certain flaws and analytic limitations. The other two tender more narrowly drawn perspectives on specific dynamics. These are glimpses, not overviews, of the regulatory landscape. Folding together insights from all three, however, offers a path toward a more perspicacious understanding of geopolitical dynamics, and the most likely path for global digital regulation.

The first of those books is Professor Anu Bradford's deeply researched and extensively documented *Digital Empires: The Global Battle to Regulate Technology*. Bradford offers a sweeping and detailed, yet still eminently readable, account of "three digital empires," or "regulatory models that provide competing visions for the digital economy," emerging from the United States, China, and the European Union.[17]

---

[15] In previous work, Justice Mariano-Florentino Cuéllar and I have drawn on Professor Robert Putnam's powerful model of international politics as a "two-level game." Cuéllar & Huq, *supra* note 10, at 336–49 (discussing Robert D. Putnam, *Diplomacy and Domestic Politics: The Logic of Two-Level Games*, 42 INT'L ORG. 427, 433–51 (1988)). The discussion in this Book Review takes Putnam's core insight—that nation-states' governments act strategically at the international and domestic level in anticipation of their interaction—as a starting point.

[16] This tension is familiar in political science work. Institutional theories of politics are characterized by "reductionism, the exogeneity of certain fundamental elements of political life, and a privileging of structure over agency," while ideational theories emphasize that "actors' understanding of their own interests is apt to evolve as the ideological setting of politics changes." Robert C. Lieberman, *Ideas, Institutions, and Political Order: Explaining Political Change*, 96 AM. POL. SCI. REV. 697, 698 (2002).

[17] ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY 23 (2023) (emphasis omitted) [hereinafter BRADFORD, DIGITAL EMPIRES].

The "three empires" trope offers Bradford a parsimonious and flexible analytic lens by which to isolate and model geopolitical dynamics so as to generate predictions of likely future policy pathways. In her pithy and memorable formulation, the United States has a "market-driven regulatory model," China has a "state-driven" model, and the European Union's approach is "distinctly rights-driven."[18] Resisting a prevailing wisdom that focuses solely upon the China–U.S. axis of conflict,[19] Bradford predicts that it will be the rights-driven EU model, not the historically regnant U.S. market-centered approach, that likely will offer the leading alternative to China's statism in the near term.[20] Even with this striking prediction in mind, *Digital Empires*'s most distinctive contribution is its more general synoptic model of geopolitical conflict, one that extends Bradford's earlier, influential work on European regulation.[21] It is a conjecture of ambition and sweep, worthy of close study.

In contrast, the two other books considered here each elevate to public attention a specific, neglected margin of geopolitical competition over digital technologies. Each can be read as suggesting that the dynamics it highlights are the truly significant, perhaps the ultimately dispositive, ones for the field of new digital technologies as a whole.

In *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, Professor Aynne Kokas offers a carefully focused polemic criticizing the way in which U.S. law's default posture of largely unregulated markets in data has facilitated the flow of vast tides of personal information to foreign states such as China.[22] She provides extensive evidence of how data initially gathered for private, commercial gain by U.S. or multinational companies tends to move to China, and thus into the potential reach of its party-state.[23] She further demonstrates that the Chinese party-state views such data as a strategic asset in

---

18 *Id.* at 7–9 (emphasis omitted).

19 *See, e.g.*, Kaveh Waddell, *The Global Race Between China and the U.S. to Set the Rules for AI*, AXIOS (July 14, 2019), https://www.axios.com/artificial-intelli-gence-china-united-states-5bea5020-c5c6-4527-8d25-7bf0036f6384.html.

20 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 21–22.

21 *See generally* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020) [hereinafter BRADFORD, BRUSSELS EFFECT].

22 KOKAS, *supra* note 8, at 2.

23 *See, e.g.*, *id.* at 165–68.

geopolitical competition, capable of being leveraged to many nebulous yet nefarious ends.[24]

In contrast to Kokas's broadly contemporaneous snapshot of U.S. markets' perverse effects, Professors Henry Farrell and Abraham Newman's *Underground Empire: How America Weaponized the World Economy* offers new reasons to nest new digital technologies into the arc of longer historical dynamics and the context of other, seemingly technologically distinct policy domains.[25] Farrell and Newman look back to the post–World War II period in which the United States obtained a large measure of geopolitical influence through its construction and control over the physical channels of transnational communication and finance.[26] They position emerging conflicts over the internet and AI as efforts to extend that Cold War equilibrium tilting in a U.S. direction.[27] Where others see novel great-power politics, they perceive the waning of an older hegemony. Newman and Farrell warn, however, that ongoing efforts by the United States to extend this Cold War "underground empire" into new digital domains will risk "a new spiral of economic confrontation" shorn of happy endings.[28]

Digital Empires, *Trafficking Data*, and *Underground Empire* each make distinctive, valuable contributions toward a more comprehensive understanding of the geopolitics of digital regulation. All three are in their way praiseworthy achievements. But in particular, Bradford's volume is to be applauded unreservedly for its breadth and synoptic ambitions. It thus offers a unique launching point for further interrogation.

Leveraging that ambition, this Book Review takes the general model of geopolitical competition of *Digital Empires* as a starting point for analysis precisely because of its comprehensiveness and parsimony. To that end, Part I offers a capsule account of the core conceptual and predictive claims of *Digital Empires*. It then tries to capture the central empirical insights of *Trafficking Data* and *Underground Empire*. In Part II, I focus closely on the ambitious three-empire typology of *Digital Empires*. By bringing that typology into conversation with the findings of Kokas,

---

[24] *See id*. at 169.

[25] HENRY FARRELL & ABRAHAM NEWMAN, UNDERGROUND EMPIRE: HOW AMERICA WEAPONIZED THE WORLD ECONOMY 2 (2023).

[26] *Id.* at 20–28.

[27] *Id.* at 8.

[28] *Id.* at 191.

Farrell, and Newman, I hope to spark some doubts about its fit and perspicacity. Part III then draws on conceptual and empirical findings of all three books to begin a sketch of digital regulation's geopolitics, one that builds on, and yet improves, *Digital Empires*'s ambitious model. Unlike Bradford, I see a more limited regulatory convergence, and not a process of competition between states that the EU is "winning" according to some uncertain criterion. This island of agreement, moreover, is tightly constrained by a churning sea of infrastructural conflict between China and the United States. As a result, I have a less optimistic view than Bradford of the likely outcomes of global regulatory jockeying over new digital technologies. Foreboding, not celebration, may well be the order of the day.

I. MAPPING GEOPOLITICAL CONFLICTS OVER DIGITAL TECHNOLOGIES

Before offering capsule summaries of the three books under consideration, one point of conceptual ambiguity should be addressed. Despite the fact that one of the three books uses the term "digital" in its title (as well as liberally throughout its text) and the other two use it extensively in their bodies, there is no clear definition of the digital in any of them. To avoid confusion, we can usefully start with a definition serviceable for all three books.

The term digital was coined in 1942 to describe a machine that solved equations rapidly using fast electrical pulses rather than with mechanical counters.[29] Evolving beyond that sense, the same term is deployed today to describe technologies that use silicon-based transistors to store, process, and deploy information. Such digital devices have been widely available since the 1960s.[30] They are so woven into the fabric of quotidian experience that they have ceased to be in any way remarkable.

To use the term digital in its original sense would plainly sweep in too much. Instead, I deploy the term digital here to capture a class of contemporary applications that rely on recent iterations of information-acquisition and -processing technologies. Core cases include social media platforms, search engines, two-sided virtual markets (such as those central to the gig economy), digital surveillance tools that match identities to biometric data

---

29 PAUL E. CERUZZI, COMPUTING: A CONCISE HISTORY 1–2 (2012).

30 JAMES W. CORTADA, THE DIGITAL FLOOD: THE DIFFUSION OF INFORMATION TECHNOLOGY ACROSS THE U.S., EUROPE, AND ASIA 3 (2012).

(such as facial and gait recognition tools), and wearable and household devices that are wired to collect and emit data about their uses and the environment. AI is the most recent addition to the digital toolkit. Obviously, this list is not exhaustive. There are many other industrial and commercial uses that receive less attention. Provided these core cases are clearly placed in view, however, the term digital can be used in what follows without seeding any unnecessary confusion.

A. The "Three Empires" Problem

Digital Empires offers a richly detailed narrative account of geopolitical conflict over digital regulation as a foundation for a crisply articulated model of transnational relations. This telling precipitates out into a series of relatively confident and crisp predictions. Precisely because of its analytic clarity and boldness, it provides a valuable starting point for analysis.

1. Competing regulatory models.

Digital Empires makes two central claims. First, it contends that current geopolitical conflicts over digital technologies can be understood in terms of competition between three ideologically distinct approaches associated with the United States, China, and Europe.[31] Second, it derives from this tripartite account a series of right and precise predictions about the trajectory of geopolitical conflict. At its core, the book proposes that the Chinese approach to digital regulation will have "continu[ed] appeal."[32] More emphatically, it predicts that the EU will also likely exert "considerable power and influence in advancing its own digital agenda," since its global adversaries have "no effective response to counter the influence that European regulations have on the conduct of tech companies."[33] The regulatory power on the wane, by process of implication, is the market-focused United States.

In contrast to a dominant strand of the literature emphasizing U.S.–China conflict over the rate of new technology acquisition,[34] Bradford draws contrasts between all these three

---

[31] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 6–11.

[32] *Id.* at 29.

[33] *Id.* at 361.

[34] *See* Graham T. Allison, *The Clash of AI Superpowers*, 165 NAT'L INT. 11, 22 (2020). *See generally* Eric Schmidt, *Innovation Power: Why Technology Will Define the Future of Geopolitics*, 102 FOREIGN AFFS., Mar./Apr. 2023, at 38; KAI-FU LEE, AI SUPERPOWERS: CHINA, SILICON VALLEY, AND THE NEW WORLD ORDER (2018).

regulatory models, highlighting ways in which they are all in competition with the other two.

Each of the book's distinctive regulatory models is explained in terms of a central organizing idea. The United States has a "market-driven" model that pivots on "protecting free speech, the free internet, and incentives to innovate."[35] China has a "state-driven model" that aims "to maximize the country's technological dominance while maintaining social harmony and control."[36] Meanwhile, the EU follows a "rights-driven . . . humancentric approach to regulating the digital economy" that is grounded on commitments to "fundamental rights," such as privacy, and "the notion of a fair marketplace."[37]

Each of these encapsulations is substantiated in seriatim chapters devoted to explicating the three models in extensive detail.[38] One of the book's great virtues, indeed, is the extensive and scrupulous accounting of policies and actions comprising the three models. Her argument respecting the United States, for example, is anchored in specific deregulatory, market-dependent measures[39] such as § 230 of the Communications Decency Act,[40] the relatively weak enforcement of national antitrust laws,[41] and public policy initiatives from the Clinton administration onwards putatively aimed at promoting global "internet freedom."[42] Bradford's Chinese model centers upon the Communist party-state's record of tight internet regulation and surveillance amounting to "digital authoritarianism."[43] It is projected beyond Chinese borders, on her account, primarily through investments in other nations as part of the Belt and Road Initiative.[44]

---

35 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 7, 33.

36 *Id.* at 9, 69.

37 *Id.* at 9; *see also id.* at 105 (adding the further goals of "preserv[ing] the democratic structures of society[ ] and ensur[ing] a fair distribution of benefits in the digital economy").

38 *Id.* at 33–145.

39 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 42–47.

40 47 U.S.C. § 230.

41 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 50–52.

42 *Id.* at 40–42, 265–69.

43 *Id.* at 70, 77–91.

44 *Id.* at 291–308 (focusing largely on the provision of physical infrastructure for digital communication and surveillance equipment). Since 2016, China has signed bilateral agreements with 140 countries for Chinese firms to provide many different kinds of physical and financial infrastructure. Sebastian Haug, *Mutual Legitimation Attempts: the United Nations and China's Belt and Road Initiative*, 100 INT'L AFFS. 1207, 1207 (2024); *see also* EYCK FREYMANN, ONE BELT ONE ROAD: CHINESE POWER MEETS THE WORLD 10 (2021) (characterizing the Belt and Road Initiative as a "hugely diverse set of overseas investment and construction projects that Chinese firms have undertaken since the early 2010s").

The European model, then, is defined in terms of the EU's regulatory record in respect to data privacy, platform-generated harms, robust competition-law enforcement, and AI harm reduction.[45] All these lawmaking projects are pitched as ample and benevolent in tenor. We are not meant to see them as reiterations, in novel forms, of older imperial desires.

In each case, moreover, Bradford is very clear that she is not making a totalizing claim about a jurisdiction's approach to digital technologies. Rather, she is identifying a central tendency. For example, she recognizes that U.S. policy is not exclusively animated by free-speech and free-market values, and that the federal government supplies funding to many firms, albeit "in a more decentralized fashion," to stimulate economic growth in suspiciously Keynesian terms.[46] Recent industrial policy under Presidents Donald Trump and Joe Biden, she notes, evinces a greater willingness to tolerate state protection for domestic digital firms than the Reagan, Clinton, and Bush administrations.[47] Similarly, China not only has its own, rather tough-minded privacy statute, the Personal Information Protection Law,[48] but has also leveraged private venture capital financing from Silicon Valley to build its domestic digital industries.[49] At the other vertex of the triangle, European nations, including Greece, Hungary, and Spain, have made "extensive" use of spyware against political opponents.[50] So much for goodness and benevolence. The force of *Digital Empires*'s modeling of geopolitical competition, in other words, does not depend on whether Bradford has demonstrated necessary features of U.S., European, and Chinese policymaking at all points: it turns on whether her identification of a central tendency is compelling.

Obviously, these starkly different models produce sparks as they rub against each other in transnational markets and at geopolitical flashpoints. In the second movement of its argument, *Digital Empires* sketches two ways in which regulatory models can clash: vertically and horizontally.[51] As the TikTok controversy

---

45 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 105–31.

46 *Id.* at 58–59.

47 *Id.* at 52–57, 212–13.

48 Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 1117.

49 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 91–93.

50 *Id.* at 143.

51 *Id.* at 6.

in the United States shows, states engage in "vertical" battles with foreign firms operating in their jurisdiction.[52] And, as the dueling export-control regimes suggest, states also compete directly in "horizontal" conflicts with each other, where firms are mere pawns in geopolitical contests between nations.[53]

Bradford suggests that vertical conflicts can "evolve" into horizontal ones.[54] But this detail is only partly supported by her account. It is true of the EU's efforts to tax technology from the United States, which spilled over into transnational negotiations over a new tax treaty.[55] But it is not a good description of U.S.–China conflicts over technological exports and 5G infrastructure, where there has been no evolution in the nature of the conflict.

Discussion of these dynamics forms a big part of *Digital Empires*'s text—in large part because Bradford is assiduously careful in documenting the twists and turns of sundry regulatory battles. But I am not sure they are central to her core argument. Instead, I read this section as connective tissue, not the beating heart, weaving together her threshold, descriptive claim about three ideologically—hence incompatible—regulatory models, with her subsequent prediction about how the tension between these models is likely to play out in the near term.[56]

The second core claim of *Digital Empires* is predictive in character: the conflicts between the three regulatory models, Bradford anticipates, will have a distinctive end state. Consistent with the dominant narrative of a resurgent Asian superpower,[57] she suggests that China will continue to press its statist (sometimes labeled "authoritarian") model with some success.[58] On this point, Bradford's argument implicitly seems to shade into familiar realist claims about the persistence, and even inevitability, of "great-power competition."[59]

---

52 *Id.* at 13–15, 149–82.

53 *Id.* at 11–13, 183–254.

54 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 183.

55 *Id.* at 238–42.

56 This section of the book, even if analytically necessary, makes no novel claim. No reasonable observer of recent global debates on digital regulation would think it novel to observe that nation-states struggle to regulate foreign companies, *see, e.g.*, Ganesh Sitaraman, *The Regulation of Foreign Platforms*, 74 STAN. L. REV. 1073, 1078 (2022), or that there is friction between great powers in respect to the shape of digital regulation, *see* Cuéllar & Huq, *supra* note 10, at 336–49.

57 *See supra* note 19.

58 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 364–66.

59 JOHN J. MEARSHEIMER, THE TRAGEDY OF GREAT POWER POLITICS 2–3 (2001) (contending that "the world is condemned to perpetual great-power competition").

But she also proposes that the European rights-centered model will become increasingly important and influential. It well may, she posits in her second prediction, eclipse the U.S. market-centered model that has dominated the post–World War II period into the early twenty-first century.[60] Thanks to "public scandals," citizens of both the United States and other democracies are increasingly "question[ing] the merits of the market-driven regulatory model."[61] As a normative matter, she conduces the European model is also the "most attractive" of those now available because it offers a happy balance between the "too permissive" U.S. and the "too oppressive" Chinese approaches.[62]

This is, indeed, a distinctive position at some distance from the conventional wisdom. In her earlier work, Bradford coined the idea of a "Brussels Effect," borrowing from a literature on the "California Effect," to characterize the adoption of European regulatory norms by non-European firms and other jurisdictions as a consequence of market inelasticities, economies of scale, and first-mover advantages.[63] What likely will result in the digital context, Bradford posits, will be a "bilateral digital world marked by continuing conflict," albeit one in which market interdependencies prevent either full, autarkic decoupling or a collapse into overt, violent conflict.[64]

Somewhat surprisingly, the ensuing prediction turns out to be less a novel patterning of global tensions than a reiteration of tendencies familiar from the latter part of the twentieth century. It is a bipolar battle in which "the strength of liberal democracy as a model of government" is put to the test by autocratic foes.[65] And what is this but the Cold War cliché of democracy versus the dictators with hashtags?[66]

---

60 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 361–63.

61 *Id.* at 363. With a surfeit of optimism that hints at a tendency to overread the evidence in light of her normative priors, Bradford calls the January 6, 2021, attacks on the Capitol a "turning point." *Id.*

62 *Id.* at 367. Bradford argues that a rights-driven model does not stifle innovation and need not be characterized by regulatory failures. *Id.* at 369–87.

63 BRADFORD, BRUSSELS EFFECT, *supra* note 21, at 25–66.

64 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 386–87.

65 *Id.* at 392.

66 *Cf.* John J. Mearsheimer, *The Inevitable Rivalry: America, China, and the Tragedy of Great-Power Politics*, 100 FOREIGN AFFS., Nov./Dec. 2021, at 48, 48 (discerning a "new cold war" between the United States and China).

2. Threshold puzzles of the "Three Empire" problem.

The tripartite "digital empires" model deserves careful attention as a leading scholar's effort to synthesize, and hence render legible, important geopolitical premises of digital regulation. On this point, *Digital Empires* is nonpareil. Neither *Trafficking Data* nor *Underground Empire* essays anything so ambitious—and so, my treatment of those books in the following Section will be more cursory.

Yet even at this threshold stage, and prior to a close examination of the book's analytic and empirical foundations, it is worth observing that the core claims of *Digital Empires* have puzzling gaps and incoherences. Setting four of these lacunae out here helps set the stage for a more careful treatment of the book's central claims in Part II.

First, notwithstanding its ambition to characterize the global context of digital regulation, *Digital Empires* is strikingly narrow in its geographical scope. It is completely focused on the "great powers" of traditional realist theory.[67] It either ignores the regulatory efforts of "smaller powers"[68] or treats them as entirely derivative of great-power machinations. To be clear, the problem is not limited to a single text. It is endemic. A crabbed vision of the "global," which cuts out Africa, Latin America, and Asia beyond China, is evident in all three books, and much of the literature on digital regulation more generally.

One would hence not know from reading the three books considered here that there are significant efforts at digital regulation emerging from Africa.[69] In 2023, for example, the African Union signed the Malabo Convention, a comprehensive data security and cybersecurity agreement.[70] Even in 2021, Professor Nathalie

---

[67] In realist theory, great powers are determined by their military capabilities. *Id.* at 50. On this view, the EU arguably does not count as a great power.

[68] *Id.* at 50.

[69] *See, e.g.*, Grace Ashiru, *Kenya Faces Backlash from Tech Community over AI Regulation Efforts*, TECH IN AFR. (Feb. 18, 2024), https://perma.cc/ER37-QCL4. For a discussion of how governments in Africa are using technology to further their political aims, see Iginio Gagliardone, *The Technopolitics of Communication Technologies in Africa*, *in* THE PALGRAVE HANDBOOK OF MEDIA AND COMMUNICATION RESEARCH IN AFRICA 263, 264 (Bruce Mutsvairo ed., 2018).

[70] African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) (June 27, 2014). For discussion, see Charles Asiegbu & Chinasa T. Okolo, *How AI Is Impacting Policy Processes and Outcomes in Africa*, BROOKINGS INST. (May 16, 2023), https://perma.cc/P4S4-DGGC. While the Malabo Convention was signed after the books considered here were likely sent to press, it was in negotiations from 2014 onward. Its absence cannot be excused by pointing to its vintage.

Smuha compiled a list of national regulatory efforts respecting AI in Japan, China, Canada, Dubai, Singapore, and Australia.[71] That list would undoubtedly be longer today. It would, for example, have to account for India's ambitious data protection law, enacted in 2023.[72]

Nor would one know that there are important spillovers from digital goods beyond the triangle of the United States, China, and Europe. Some of these are negative. Much of the training of AI models, for example, is performed by African workers, who decry the mental health effects of having to grapple with constant streams of graphic and violent imagery.[73] Some are positive in nature. Africa, for example, is also the youngest, fastest-growing continent. It will likely be called home by a quarter of humanity by 2050.[74] Given such trends, this ought to be a moment of exciting possibilities for African nations. To be sure, many in that continent lack access to digital media as a consequence of "[c]olonial communication policies" that have shaped "networks for media consumption and distribution."[75] But Africa will also contain the world's largest growing markets of digital consumers—markets that ought to be able to exert their own regulatory demands on digital firms.

This failure to consider Africa (and much else of the world beyond the supposed superpowers) by the books considered here reflects a dubious form of myopia. It obscures important transnational dynamics, such as the reproduction of colonial-era dynamics of exploitation within digital economies, that warrant more

---

71 Nathalie A. Smuha, *From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence*, 13 LAW, INNOVATION & TECH. 57, 75–76 (2021).

72 Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 3, 2023), https://perma.cc/NN9V-QMY3.

73 Niamh Rowe, *'It's Destroyed Me Completely': Kenyan Moderators Decry Toll of Training of AI Models*, THE GUARDIAN (Aug. 2, 2023), https://perma.cc/4JU7-ZVR3; Billy Perrigo, *Exclusive: OpenAI Used Kenyan Workers on Less than $2 Per Hour to Make ChatGPT Less Toxic*, TIME (Jan. 18, 2023), https://perma.cc/3A8A-FMDW.

74 Declan Walsh, *The World Is Becoming More African*, N.Y. TIMES (Oct. 28, 2023), https://www.nytimes.com/interactive/2023/10/28/world/africa/africa-youth-population.html. Bradford does discuss Chinese policy in Africa—but treats African nations as hapless objects of Chinese power and not as sovereign agents in their own right. BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 297–300.

75 PAYAL ARORA, THE NEXT BILLION USERS: DIGITAL LIFE BEYOND THE WEST 53 (2019).

serious attention.[76] And it conduces to descriptive claims that, while strictly true, may well mislead in context.[77]

In a sense, the problem here is an old and familiar one. A cavalcade of scholarly depictions of the "international order" over the centuries have helped themselves to an assumption of "European exceptionalism" and a high-handed belief that, surely, the European "vocation" is to act as "a political archetype for the rest of the world."[78] Rather than eschewing this historical myopia, *Digital Empires* in particular offers a normative vision that maps closely onto that familiar historical hierarchy. Its curtailed field of vision is a near-reflexive (albeit perhaps hardly conscious) recapitulation of the cramped and parochial Eurocentric vision that has historically characterized much international law scholarship.[79] One might have hoped that contemporary theorists so palpably enamored of the future would overcome the problematic blind spots of the past and not rehearse them once more for the digital age.

Second, there are a number of opacities in *Digital Empires*'s predictions about convergence upon the rights-driven model and bilateral conflict with the state-driven model. I draw out three such ambiguities here but return to them in Part II, which closely scrutinizes the book's claims.

As a threshold matter, the exact nature of the predicted policy convergence is ambiguous. It might be understood as a claim that democratic nations will emulate the specific regulatory measures advanced by the EU. Or it might be a prediction that those nations will adopt more extensive regulatory frameworks for digital technologies, albeit not necessarily ones that echo or borrow from EU law.

---

76 *See, e.g.*, KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 254 n.58 (2021).

77 For example, *Digital Empires* claims that the EU's "proposed AI regulation is the first of its kind globally." BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 115. But other jurisdictions had made substantial moves toward comprehensive AI regulation at roughly the same time that the EU did. In January 2019, Singapore released a "Model AI Governance Framework." *Model Artificial Intelligence Governance Framework: Second Edition*, PERS. DATA PROT. COMM'N OF SING. (Jan. 21, 2020), https://perma.cc/8DP2-MKE6. The Parliament of Canada has been discussing a comprehensive statute on AI since 2022; it remains in committee as of this writing. *AI Watch: Global Regulatory Tracker—Canada*, WHITE & CASE (May 13, 2024), https://perma.cc/U94M-XAEN. A broader geographic focus might have led Bradford to avoid strained factual assertions.

78 Jennifer Pitts, *Empire and Legal Universalisms in the Eighteenth Century*, 117 AM. HIST. REV. 92, 94 (2012).

79 *See id.* at 98 (explaining how early theorists of international law "saw the European order they were codifying as the basis for a future international order").

Unfortunately, Bradford equivocates between these two possibilities. The effect of this wavering is to render her overall predictive claims more than a little opaque. On the one hand, she explicitly asserts that she is extending her work on the Brussels Effect by asserting that EU law will spill over because other jurisdictions will be "inspired by" or will "emulate[ ]" the particular measures adopted in Europe.[80] On the other hand, her argument for convergence rests on the idea that democratic nation-states, including the United States, will abandon a deregulatory posture and simply evince greater willingness to regulate in general.[81] They are doing so not because of market inelasticities, economies of scale, or first-mover advantages: rather, Bradford suggests, they are doing so because the market-driven model has lost its credibility.[82] Yet if that is so, then there is no particular reason why EU law should be a template for other governments.[83] There are surely many ways to regulate digital technologies, and the European approach may not always be the best fit for a given nation.

Because *Digital Empires* does not offer a truly global treatment of digital regulation, it is very hard to tell which of these accounts is more consistent with a comprehensive tally of the evidence. At least some examples left off the page, however, point toward the latter view. The African Union's Malabo Convention, for example, "combine[s] cybersecurity, security of electronic transactions[,] and personal data protection" in a way that does not track EU law on all, or even most, points.[84] But an enterprising analyst might find enough echoes to claim a medal for the Brussels Effect.

A second and related ambiguity concerns the exact nature of the predicted regulatory convergence among democratic nation-states. It seems to be a premise of the predictive claim of *Digital Empires* that the rights-driven, market-driven, and state-driven

---

80 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 335; *id.* at 324–26 (explaining the Brussels Effect on terms of emulation of specific European laws).

81 *See, e.g.*, *id.* at 351 ("[E]ven the US may now be inching toward the European rights-driven approach.").

82 *Id.* at 361–64 (charting the "[d]ecline" of the market-driven model).

83 Bradford argues that companies will conform to EU regulations in "an effort to standardize their products and services worldwide." *Id.* at 28. But this raises the question why European law, and not African or Chinese law, would be the focal point for convergence.

84 Nnenna Ifeanyi-Ajufo, *The AU Took Important Action on Cybersecurity at Its 2024 Summit—But More Is Needed*, CHATHAM HOUSE (Feb. 23, 2024), https://www.chathamhouse.org/2024/02/au-took-important-action-cybersecurity-its-2024-summit-more-needed; *see also* African Union Convention on Cyber Security and Personal Data Protection, *supra* note 70.

models of regulation are mutually exclusive. You cannot have more than one. The market-driven model must be abandoned for the rights-driven model to take hold, or vice versa. And it seems that neither of those models can be sustained alongside a pursuit of the state-driven model. Stated a bit more strongly, the assumption seems to be that *Digital Empires*'s three regulatory models are mutually incompatible, such that it is not feasible for a jurisdiction to find ways to advance state power, build markets, and advance the individual rights-like interests of its citizenry all at the same time. As we shall see, this assumption is not entirely earned.

Bradford's predictive thesis, in a final ambiguity, slices the regulatory world into two parts and assumes all of the components of a part move in unison, but at a different tempo from the other part. That is, she seems to assume that different digital policy domains move at least in rough unison, but that they are also independent of other policy domains. Hence, *Digital Empires* addresses a very wide array of transnational conflicts. It deals, for example, with disputes over content moderation,[85] privacy,[86] the specifications of physical communications infrastructure,[87] taxation,[88] transnational data flow,[89] and industrial policy.[90] Its prediction of movement from the market-driven to the rights-based model appears to assume that all of these different kinds of policy are going to move in a kind of lockstep. From a different vantage point, however, *Digital Empires* considers only a narrow slice of geopolitical disputes and excludes the historically most potent ones. Bradford only glancingly addresses the possibility that geopolitical differences in other domains (say, territorial conflicts over Ukraine or Taiwan) shape digital policy. In particular, she does not account for the possibility that "[s]tructural changes around energy and finance" are driving geopolitical tumult.[91] (Energy and finance, indeed, play no meaningful role in her account.) That is, the digital domain is assumed to be both internally homogenous such that it moves in lockstep, but also sufficiently distinct from other domains of geopolitical conflict to

---

85 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 43.

86 *See, e.g.*, *id.* at 7–8.

87 *See, e.g.*, *id.* at 290–91.

88 *See, e.g.*, *id.* at 126.

89 *See, e.g.*, *id.* at 19–20.

90 *See, e.g.*, BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 134–35.

91 HELEN THOMPSON, DISORDER: HARD TIMES IN THE 21ST CENTURY 5 (2022).

warrant separate treatment. These assumptions, however, are neither stated nor justified.

Third, while acknowledging deviations from these regulatory ideals,[92] *Digital Empires* posits ideas as the engine driving national and supranational policymaking. Its three regulatory models are ideational rather than institutional in character, insofar as they do not rest on any account of states' internal political economy, the relative power of state versus private actors, or the play of forces between interest groups. Bradford's implicit premise seems to be instead that the United States, China, and the EU are motivated by an ideological commitment to a certain style of regulation. These favor respectively the market, the state, and the individual, respectively. To the extent they act as states in the geopolitical domain, moreover, their decisions can be glossed in terms of allegiance to a single idea about *regulation* as such—rather than, say, an idea about the proper role of a nation on the world stage.

It is worth asking whether this assumption is persuasive. There is, to be sure, a rich political science tradition demonstrating that ideas do matter. In a recent magisterial history of the twentieth-century state, for example, Professor Charles Maier has argued that many of the most successful nation-state leaders of the twentieth century possessed a "self-aware ambition" in the form of what he called a nation-state's historical "project," to advance an agenda "going far beyond ordinary administration" and "consciously [ ] to inflect the course of history."[93] For great powers, this had not just domestic policy implications, but drove efforts to make a world hospitable for their values—values that were often cast in "universalist" terms.[94]

Bradford's ideational framing, and her eschewal of materialist motivational models, raises a number of questions without easy answers. To begin with, it assumes that the ideas asserted by a nation-state's leaders can be taken as a more reliable guide to motivations than the specific interests and institutional structures of representation and power that make up the nation-state. It also assumes that key actors have not just specific ideological commitments, but also the incentives and opportunities to

---

92 *See supra* text accompanying notes 46–50.

93 *See* CHARLES S. MAIER, THE PROJECT-STATE AND ITS RIVALS: A NEW HISTORY OF THE TWENTIETH AND TWENTY-FIRST CENTURIES 5–6 (2023).

94 *See id.* at 7; *id.* at 387 ("The project-state was at its best a twentieth-century device for advancing what might be called the common good.").

translate these into actions within a given domestic political system.[95] *Digital Empires*, however, generally leaves open the question of how "ideational variables influence political behavior" on the ground within nation-states.[96] We are rather asked to accept on faith that they do.

The question of how ideas elicit changes in political behavior is especially sharply presented by its prediction that nation-states will learn from the "public scandals" of U.S. tech companies and move toward a rights-oriented regulatory model.[97] This claim of learning from observed experience, and shifting from market-driven to rights-driven regulatory models, implies that ideological commitments are not fixed. It suggests that they are instead mutable in the teeth of new, contrary evidence. But this assumption is not obviously in harmony with the book's threshold premise that *fixed* ideas about the state, the market, and the rights-bearing individual (as opposed to interests) decisively shape a nation-state's approach in the first instance.

Fourth, perhaps most importantly, the emphasis on ideas obscures certain brute facts of global material competition. *Digital Empires*'s talk of tripolar competition blinks the fact that global *power* along many dimensions "remains nearly unipolar."[98] The United States exercises largely unchallenged "military dominance over the world's major hydrocarbon reserves."[99] Its Navy has "global reach,"[100] whereas China has at times struggled against minor powers such as the Philippines and Indonesia even in its maritime backyard.[101] The United States also has

---

95 Lieberman, *supra* note 16, at 698.

96 Sheri Berman, *Ideas, Norms, and Culture in Political Analysis*, 33 COMP. POL. 231, 233 (2001).

97 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 362–63.

98 TOM STEVENSON, SOMEONE ELSE'S EMPIRE: BRITISH ILLUSIONS AND AMERICAN HEGEMONY 1–2 (2023).

99 *Id.* at 2.

100 *Id.*

101 Agnes Chang, Camille Elemia & Muyi Xiao, *China's Risky Power Play in the South China Sea*, N.Y. TIMES (Sept. 15, 2024), https://www.nytimes.com/interactive/2024/09/15/world/asia/south-china-sea-philippines.html; Joe Cochrane, *Indonesia, Long on Sidelines, Starts to Confront China's Territorial Claims*, N.Y. TIMES (Sept. 10, 2017), https://www.nytimes.com/2017/09/10/world/asia/indonesia-south-china-sea-military-buildup.html. That said, the modernization of the People's Liberation Army Navy has arguably come close to matching U.S. resources in the maritime sphere. *See In Some Areas of Military Strength, China Has Surpassed America*, THE ECONOMIST (Nov. 4, 2024), https://www.economist.com/china/2024/11/04/in-some-areas-of-military-strength-china-has-surpassed-america.

"overwhelming power" over the global financial system.[102] The absence of these central facts of geopolitics from *Digital Empires* raises concerns about whether its predictions will have meaningful traction—concerns to which I will return several times below.

It follows from this last observation that Bradford's prediction of "continuing conflict" in the form of a new Cold War is undermotivated.[103] *Digital Empires* never explains why the United States and China are at loggerheads; the former's geopolitical dominance, against which the latter now chafes, is taken for granted. Nor does *Digital Empires* say why this conflict will get worse. The bare fact of ideological difference is not a sufficient explanation, for there is no reason to think that just because two states have different value systems, they must necessarily come into conflict. On this key point, her prediction rests on nebulous motivational springs bubbling up from beyond the borders of the digital.

B. Hidden Fronts in the Geopolitical Struggle over Digital Technology

Trafficking Data and *Underground Empire* offer no comparably ambitious or extensive account of the global dynamics of digital regulation. More modest than *Digital Empires*, each picks out a specific salient of such conflicts and then mines that dynamic closely. For present purposes, I offer here abbreviated summaries (and some criticism) of those claims, so they can be deployed as foils for testing *Digital Empires*'s tripartite model. By doing so, I hope to move toward a more perspicacious understanding of the geopolitics of digital regulation.

1. How democracies leak data.

Trafficking Data homes in upon one element of the U.S.–China interaction: the one-way flow of personal data generated through commercial activity in the former to companies closely aligned to the Chinese state, or to the state itself. Kokas defines "data trafficking" as the one-way flow of data from democratic jurisdictions to China across national boundaries where it can "become subject to new forms of control that further alienate it from any existing protections" that guard individuals' privacy and

---

[102] Tom Stevenson, *First Recourse for Rebels*, LONDON REV. BOOKS (Mar. 24, 2022), https://perma.cc/9DA5-TP4L.

[103] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 387.

autonomy.[104] This is distinct from and in contrast to what she calls "data migration," which occurs through "reliable, transparent" mechanisms such as the legal arrangements that govern the flow of personal data from the EU to the United States.[105] Trafficking is distinctive in the extent to which the transfer of data to the Chinese state, or entities within its effective control, is neither anticipated nor authorized by those who produce it.

The signal contribution of *Trafficking Data* is to show that the data-security concerns animating the TikTok ban[106] are structural and pervasive in nature, and not unique to one particular country or one species of digital technology. In this vein, it showcases the manifold ways in which a weakly regulated digital economy organized around the aggressive extraction and monetarization of data can be exploited by authoritarian states. On one side, the relatively weak regulatory "multistakeholder"[107] structures of U.S. digital markets mean that firms can collect large amounts of data with relatively few legal frictions.[108] On the other side, it is not just Chinese ownership of firms such as TikTok that generates data trafficking, but a wider array of market mechanisms that conduce to the unauthorized flow of data to Chinese entities. These Chinese tech firms, Kokas argues, may be private in form, but should also be understood as "vehicle[s] for economic statecraft."[109]

Central to Kokas's story is the transnational market for corporate control through mergers, acquisitions, and other deals. When U.S. firms form joint ventures with Chinese entities in order to enter the Chinese market, they traffic data to China.[110] When Chinese venture capital purchased the dating app Grindr,[111] or when the Chinese firm Haier bought GE Appliances,[112] it resulted in the trafficking of intimate data extraterritorially.[113] When the Chinese firm WuXi AppTec acquired NextCODE Health, it enabled the

---

104 KOKAS, *supra* note 8, at 8–9.

105 *Id.* at 13. This legal structure is closely analyzed in Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 118–19, 160–64 (2017).

106 *See supra* text accompanying note 1.

107 KOKAS, *supra* note 8, at 16.

108 *Id.* at 15–17; *id.* at 23 (noting the absence of a single regulator of data privacy in the United States); *id.* at 189 ("The flexible US tech regulatory landscape facilitates data extraction by Chinese firms.").

109 *Id.* at 7.

110 KOKAS, *supra* note 8, at 46.

111 *Id.* at 47.

112 *Id.* at 177–79.

113 For some readers, Kokas's discussion of the trafficking of data from baby monitors and sex toys is especially disconcerting. *Id.* at 180–85.

"gathering [of] genomic material" for transfer to China.[114] When the Chinese national champion Tencent purchased significant stakes in game makers Epic Games (creator of Fortnite) and Activision Blizzard (maker of World of Warcraft), data trafficking ensued once more.[115] When Alipay or WeChat Pay is used to transfer funds across borders, data flows to China.[116] And so on.

Hence, while critics of TikTok may be correct to say that the platform enables the unintended transfer of personal data to Chinese servers, Kokas powerfully demonstrates that it is myopic (and perhaps prejudiced[117]) to think that this problem arises solely from the fact of Chinese ownership: it is a paradoxical effect of a free-market system operating concurrently with, and in geopolitical competition against, a more state-centered and authoritarian one.

In the domestic context, the unauthorized use of data is often criticized on dignitary grounds.[118] The fear is that it can allow the state to police people's intimate lives and decision-making in ways that arguably raise profound autonomy and dignity concerns.[119] For Kokas, however, data trafficking is problematic because of its large-scale effects on geopolitical interests, and not simply for the ways it infringes upon specific individual interests. Canvassing the effects of data trafficking, she thus suggests that "China's growing influence in the tech sphere propagates illiberal digital practices."[120] Alas, she gives few specific examples of this.[121] More concretely, and so more persuasively, she contends that data aggregates obtained through trafficking act as geostrategic

---

114 *Id.* at 165–69.

115 KOKAS, *supra* note 8, at 120, 122–26, 130–32. Activision was later sold to Microsoft. *Id.* at 130.

116 *Id.* at 141; *see also id.* at 148 (noting how U.S. regulators prevented the Chinese acquisition of MoneyGram International).

117 *Id.* at 4–5.

118 *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 522 (2019) (contending that the "bare facts" of surveillance capitalism demean human dignity).

119 For example, in relation to reproductive choices, see Aziz Z. Huq & Rebecca Wexler, *Digital Privacy for Reproductive Choice in the Post-*Roe *Era*, 98 N.Y.U. L. REV. 555, 569–70 (2023).

120 KOKAS, *supra* note 8, at 19.

121 She discusses private censorship of Chinese democracy activists at China's request. *Id.* at 1–2. But this incident turned on firms' wish to maintain Chinese market-share, not data trafficking.

resources.[122] Data on how first-person shooter games are used, for example, can be used for training military AI.[123] Genomic data aggregates help build precision medicine tools that will occupy key junctions in medical supply chain, reassigning national "advantage in the critical field of health security."[124]

As with *Digital Empires*, several facets of the analytic framework developed in *Trafficking Data* are not fully worked out. To begin with, Kokas draws a sharp line between the "extensive . . . data-gathering practices" of the Chinese government[125] and the unauthorized U.S. extraction of data from other jurisdictions.[126] Yet, the flow of personal data from the EU to the United States arguably raises geopolitical concerns tempered only by the extent to which the two jurisdictions do not (yet) perceive themselves as being in intense strategic competition.[127] The 2018 Clarifying Lawful Overseas Use of Data Act[128] (CLOUD Act), for example, requires U.S.-based service providers to "preserve, backup, or disclose" electronic communications content, even when it is stored overseas.[129] These commands are arguably in tension with the data sovereignty of foreign nations that are housing servers.[130] Counterbalancing such developments is the emergence of increasingly "efficient technological end-runs available for the rest of the world that permit non-U.S. cloud customers to avoid U.S. rules

---

122 *Id.* at 188 ("When combined, [ ] data offers the Chinese government tools for setting long-term pathways for such goals as establishing global AI standards, surveilling DNA, and controlling critical infrastructure.").

123 *Id.* at 120–21.

124 *Id.* at 157.

125 KOKAS, *supra* note 8, at 94.

126 *See* FARRELL & NEWMAN, *supra* note 25, at 46–49 (documenting such extraction); *see, e.g.*, Josh Levs & Catherine E. Shoichet, *Europe Furious, 'Shocked' by Report of U.S. Spying*, CNN (July 1, 2013), https://perma.cc/4MVE-5H9U. Kokas only briefly mentions these practices but does not address their extraterritorial dimension. *See* KOKAS, *supra* note 8, at 3, 16.

127 *But see* FARRELL & NEWMAN, *supra* note 25, at 121–29 (describing European hostility to U.S. sanctions on Iran under the Trump administration).

128 Pub. L. No. 115-241, 132 Stat. 1213 (2018) (codified as amended in scattered sections of 18 U.S.C.).

129 *Id.* § 103(a)(1), 132 Stat. at 1214. It also envisages bilateral executive agreements to expedite law enforcement cooperation. *See* Rebecca Wexler, *The CLOUD Act and the Accused*, KNIGHT FIRST AMENDMENT INST. AT COLUM. UNIV. (July 19, 2022), https://perma.cc/T69Q-K3H7.

130 *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1082–86 (2017) (developing this argument from sovereignty).

for data stored outside the United States."[131] That is, the legal landscape sculpting transnational data flows is more complex (and becoming even more opaque) than Kokas allows.

In addition, as Kokas acknowledges, the perception that China presents a geopolitical threat has reoccurred periodically in U.S. history, often accompanied by racialized or xenophobic undertones.[132] She invites, but does not answer, the question whether data trafficking to China should be understood as a grave national security concern or a mere annoyance. Presumably, this depends on whether one construes the current tension with China as structural or merely psychologically deviant.

Finally, the structural nature of Kokas's critique raises questions as to the adequacy of legal remedies and interventions that do not address the equally structural weaknesses of the commercial data environment in the United States. Kokas hence offers some incremental remedial measures that could stanch the exfiltration of data to China.[133] But then, in praising EU and Japanese data protection laws, she rightly raises the question whether it is possible to address data trafficking without wholesale changes to the manner in which data flows though the commercial sector in the United States.[134] Stated in sharper terms, it is not clear that there is a remedy for data trafficking short of wholesale decoupling not just of the data-centered economy, but of capital markets more generally, between China and the rest of the world.

2. How histories of geopolitical conflict accrete.

Written for a broader, popular audience, *Underground Empire* offers a more anecdotal and informal, albeit no less forceful, perspective on the geopolitics of digital regulation. Its central claim sounds in a historical register. It is that the Cold War–era United States built a global network of "fiber-optic networks, financial systems, and semiconductor supply chains" that all "converge on the United States."[135] What on the surface appears an open internet and a borderless market for capital, Farrell and

---

131 Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1684 (2018) (describing the technological protections available for non-U.S. cloud customers); *see also id.* at 1718–20 (same).

132 KOKAS, *supra* note 8, at 4–5; *see also* Jia, *American Law*, *supra* note 2, at 655–60 (discussing historical patterns of U.S.–China conflict).

133 KOKAS, *supra* note 8, at 191–205 (proposing a series of largely incremental reforms to slow data trafficking flows under the rubric of "data stabilization wedges").

134 *Id.* at 20.

135 FARRELL & NEWMAN, *supra* note 25, at 3.

Newman propose, is in fact a "subterranean imperium" that has increasingly enabled the United States to "spread its influence across the borders of other countries, gathering information, interdicting goods, and cutting entire countries out of the global economy."[136]

As they explained in an earlier article developing similar themes, the private creation of global networks means that some states are able to leverage their control over central nodes (or the firms that control those nodes) of the global economy to impose asymmetrical costs on others.[137] This is called "weaponizing interdependence."[138] And the United States has, until now, been the chief beneficiary.

Underground Empire draws attention to three entrenched and functionally obdurate global networks over which the U.S. exercises asymmetrical power.[139] First, Farrell and Newman highlight the large degree of U.S. control over global digital communications thanks to the fact that most telecommunications data flows though routing stations physically located in the United States.[140] Centered in Northern Virginia, many were built by the American MCI WorldCom.[141] All these networks were leveraged by the National Security Agency for warrantless surveillance after the September 11 attacks.[142] The U.S. government has also exerted pressure on U.S.-based firms such as Microsoft to cooperate in geopolitical struggles, for example by leveraging its networks to aid Ukraine against Russian aggression.[143]

Second, *Underground Empire* is a testament to U.S. power over global finance. In the 1970s, U.S. financial firms led by Citibank built the Eurodollar market and a "global payments system" that influenced global financial flows.[144] Partly as a result of

---

136 *Id.* at 6.

137 Henry Farrell & Abraham L. Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L SEC. 42, 44–45 (2019).

138 *Id.* at 46.

139 FARRELL & NEWMAN, *supra* note 25, at 213 ("There is no visible exit from the underground empire.").

140 *Id.* at 9 (noting that by 2002, less than 1% of global internet traffic did not pass through the United States).

141 *Id.* at 31–38.

142 *Id.* at 46–60.

143 *Id.* at 159–61 ("As governments began to weaponize markets, not just regulate them, Microsoft found it increasingly hard to keep professing neutrality.").

144 FARRELL & NEWMAN, *supra* note 25, at 19–20, 25–28; *see also id.* at 64 (noting that "[i]f [the Society for Worldwide Interbank Financial Telecommunications] threatened to move its data overseas, Treasury could threaten the members of its governing board").

the Eurodollar market that kindled in the 1950s, "the dollar became a global currency."[145] The United States and aligned states are able to leverage their asymmetrical influence over the global network of firms managing the dollar economy to pursue geopolitical ends.

For example, the Treasury Department can designate a foreign bank such that neither U.S. financial firms nor any foreign firms that need to clear transactions in U.S. dollars will be willing to deal with them.[146] That designation power has been widely used to shape international affairs. In 2012, for example, the United States and EU pressured the Society for Worldwide Interbank Financial Telecommunications (SWIFT) into "cutting Iranian banks out of the global payments system."[147] In the wake of the February 2022 Ukraine invasion, the United States and EU froze $600 billion in reserves of the Russian central bank that were maintained at other central banks and the Bank for International Settlements.[148] In June 2024, the G7 nations agreed to use the interest earned on these frozen Russian assets to lend Ukraine $50 billion.[149] In 2022, the same power was deployed against a cryptocurrency "mixer" by designating an "inextricable part" of the Ethereum blockchain.[150] The outer limit of the designation power, it seems, has yet to be reached.

Third, the United States has leveraged its role as supplier of intellectual property and a digital marketplace to press private tech firms into its geopolitical struggles. Hence, the U.S. export-control regime enforced by the Department of Commerce allows the U.S. government to shape the behavior of "foreign-based

---

145 *Id.* at 23. Farrell and Newman do not explore the advantages accruing to the United States from dollar predominance. But these are "considerable." BARRY EICHENGREEN, EXORBITANT PRIVILEGE: THE RISE AND FALL OF THE DOLLAR AND THE FUTURE OF THE INTERNATIONAL MONETARY SYSTEM 3 (2011). U.S. buyers, for example, save transaction costs when purchasing from overseas, and other nations expend "real resources" for the privilege of obtaining dollars. *Id.*

146 FARRELL & NEWMAN, *supra* note 25, at 68.

147 *Id.* at 75; *see also id.* at 81 (noting how this power was used to pressure Huawei's bank, HSBC, to hand over financial data about the Chinese firm). Iran was temporarily readmitted to SWIFT under the so-called Iran deal. *Id.* at 116–19.

148 *Id.* at 138–39.

149 Deepa Shivaram, *G7 Agrees to Loan Ukraine $50 Billion from the Interest on Frozen Russian Assets*, NPR (June 13, 2024), https://perma.cc/KWR7-P23S.

150 FARRELL & NEWMAN, *supra* note 25, at 183–84; *see also U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. DEP'T OF THE TREASURY (Aug. 8, 2022), https://perma.cc/Q5MJ-CCKK. A mixer is in effect an app for disguising the province of cryptocurrency transactions.

technology companies that significantly touch[ ] U.S. intellectual property, even indirectly."[151]

In March 2021, the Department of Commerce implicitly threatened to use its authority[152] under the Defense Production Act.[153] It pressured the Taiwanese chip manufacturer, Taiwan Semiconductor Manufacturing Company (TSMC), into handing over information on its customers, including firms located in China, to the federal government.[154] While it is based in Taiwan, TSMC is practically "dependen[t] on U.S. intellectual property, U.S. suppliers, and the U.S. market," and so had little choice but to comply.[155]

The United States' increasing leverage of its underground empire, Farrell and Newman conclude, risks increased decoupling of the global economy. In response to the flexing of U.S. power, other nations seek to initiate costly countermeasures, and even come into outright armed conflict.[156] An early example is China's efforts through Huawei to build a 5G network insulated from U.S. influence.[157] The risks of conflict are especially acute today, Farrell and Newman reason, because neither China nor the U.S. has a framework for thinking strategically about the weaponization of commercial infrastructure akin to the game-theoretical models developed during the Cold War for managing thermonuclear conflict.[158]

In these ways, *Underground Empire* directs attention to a theater of geopolitical competition that both *Digital Empires* and *Trafficking Data* largely overlook. Kokas is explicitly concerned only with data flows and talks primarily of personal data. Purporting to apply a broader, more comprehensive lens, Bradford largely discusses the ex ante regulation of commercial actors in

---

151 FARRELL & NEWMAN, *supra* note 25, at 102.

152 Section 705 of Defense Production Act authorizes the President to "obtain information [from] . . . the United States industrial base to support the national defense." 50 U.S.C. § 4555(a).

153 Pub. L. No. 81-774, 64 Stat. 798 (1950) (codified as amended in scattered sections of 50 U.S.C.).

154 FARRELL & NEWMAN, *supra* note 25, at 168. The request was made in the form of a request for public comment from the Bureau of Industry and Security. *See* Notice of Request for Public Comments on Risks in the Semiconductor Supply Chain, 86 Fed. Reg. 53,031 (Sept. 24, 2021).

155 FARRELL & NEWMAN, *supra* note 25, at 169.

156 *Id.* at 191–93 (anticipating a "new spiral of economic confrontation" that may "tear the global economy apart or even pull the world into actual war"); *id.* at 206 (describing a "dangerous feedback loop" driven by a "dynamic of mutual fear").

157 *Id.* at 85–87, 192.

158 *Id.* at 207. One may, however, be skeptical that game-theoretical models were a causally significant factor in avoiding Cold War conflict. Perhaps luck mattered more.

the data sphere; her discussion of infrastructural power is limited to some mentions of China's Belt and Road Initiative, and entirely overlooks the global financial networks that Farrell and Newman highlight.[159] Whether Belt and Road increases China's influence on other countries' domestic policies, however, remains uncertain.[160] The historical analysis of *Underground Empire* also places Kokas's account of data trafficking in a fresh light: given that the United States has already occupied the commanding heights so far as communications and financial infrastructure go, China's effort to accumulate data as a resource might be understood as a late starter's effort to carve out a measure of countervailing power against a global hegemon that is plainly and inevitably concerned with its own interests above all else.[161] China, that is, is simply trying to catch up.

Yet Farrell and Newman's thesis also benefits from certain qualifications. For example, they largely assume that hegemonic states are able to exercise close control over the firms located at critical nodes of the global economy.[162] These firms, however, might have sufficient market power and globalized presence that they are able to resist such pressure by presenting themselves as functionally autonomous of any state's wishes.[163] Developing a variation of that idea, Professors Iain Hardie and Helen Thompson have argued that the predominant role of European banks in providing global intermediation services for dollars in practical effect "forced" the U.S. Federal Reserve to act as a lender of last resort

---

159 *See* BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 291–308. Indeed, Farrell and Newman provide a more lucid explanation of U.S. concerns about the Chinese telecommunications firm Huawei: U.S. worries are not motivated by a worry about spying, but a concern that China might build "the basic infrastructure for the world's 5G networks" and hence come to wield a new form of hegemonic power. FARRELL & NEWMAN, *supra* note 25, at 90.

160 For one thing, there are now "at least 57 countries with outstanding debt to Chinese state-owned creditors," a scale of indebtedness that raises real questions about how China manages the ensuing delicate relations. Simone McCarthy, *Developing Countries Owe China at Least $1.1 Trillion—and the Debts Are Due*, CNN (Nov. 13, 2023), https://perma.cc/42GU-737D.

161 *Cf.* FARRELL & NEWMAN, *supra* note 25, at 14 (noting that China has been "struggling to displace" U.S. hegemony over communications and financial networks).

162 *See, e.g.*, *id.* at 43–44 (arguing that "the United States could potentially use the semiconductor supply chain to threaten other countries" because "[t]he most sophisticated design companies . . . were based on U.S. soil").

163 For evidence that this occurs in the market for undersea telecommunications cables, see Lars Gjesvik, *Private Infrastructure in Weaponized Interdependence*, 30 REV. INT'L POL. ECON. 722, 737–39 (2023).

to those non-U.S. financial firms during the 2008 financial crisis.[164]

Technological innovation might also disrupt the relative market shares of firms at the nodes of global networks. This might destabilize the possibility of weaponizing these interdependences. The recent emergence of new digital channels for cross-border fiscal flows, it has been argued, may in this vein make it "increasingly difficult" for national authorities to wield influence through regulation.[165]

These possibilities do not necessarily undermine the general force of Farrell and Newman's argument. Rather, they point to the fragility of the institutional conditions under which existing forms of interdependence can be weaponized, and the pressure this creates in new policy domains—including in the digital domain—to carve out workarounds.

In these ways, the infrastructure of global communication and finance may be becoming just a little less vulnerable to weaponization by either the United States or its adversaries than the pessimistic perspective of Farrell and Newman allows.

* * *

Read together, *Digital Empires*, *Trafficking Data*, and *Underground Empire*, offer a more comprehensive account of the geopolitics of digital regulation than any one volume alone. The second pair of books also offers reasons for inflecting Bradford's more comprehensive and ambitious theory of geopolitical competition. *Trafficking Data*, for example, underscores the ways in which a national strategy can be beset by unravelling internal tensions or contradictions. *Underground Empire*, in contrast, historicizes by treating current conflicts over digital technologies accounting for the ways that they extend, or complicate, what Charles Maier has called a nation-state's "project."[166] These books suggest that by reading present digital conflicts in this historical context, with awareness of the internal tensions of each "empire," the present conjunction can come into better focus.

---

[164] Iain Hardie & Helen Thompson, *Taking Europe Seriously: European Financialization and US Monetary Power*, 28 REV. INT'L POL. ECON. 775, 776–77 (2021).

[165] Eswar Prasad, *How Will Digital Technologies Influence the International Monetary System?*, 39 OXFORD REV. ECON. POL. 389, 392 (2023).

[166] MAIER, *supra* note 93, at 5–6.

II. IS GEOPOLITICAL COMPETITION A "THREE EMPIRES" PROBLEM?

Armed with a comprehensive tally of these diverse strands of geopolitical conflict over digital regulation, it is possible to reconsider *Digital Empires*'s central tripartite model.

Recall that the three-empire model is premised on the claim that the United States, China, and Europe are locked in a fundamentally ideological battle between three regulatory models: the market-driven, state-driven, and rights-based alternatives. Moreover, it predicts that a bipolar conflict between the rights-based and the state-based models will in the end emerge from this triangular conflict. Neither of these claims, in my view, is ultimately compelling. Although *Digital Empires* offers a powerful and far-reaching account of geopolitical conflict over digital regulation, the general model that it derives from that material has meaningful limits, and its predictions are as a result incomplete.

I develop this argument in three steps. To begin with, I consider ways in which the accounts tendered in *Trafficking Data* and *Underground Empire* at a very general level fit alongside the three-empire model and its predictions. This analysis brings to light both complementarities and tensions. Next, drawing on the empirical detail offered in all three books, I closely scrutinize the idea of three regulatory models providing ideological touchstones for three empires, finding reasons for skepticism. Finally, I reconsider the force of Bradford's prediction about the triumph of Europe's rights-driven model.

A. The Confluence of Global Digital Conflicts

At a very general level, the conflicts over data and infrastructure presented in *Trafficking Data* and *Underground Empire* seem to complement and deepen Bradford's claims, albeit in complex ways.

Kokas's argument about the exfiltration of commercial data from the United States to China adds important nuance to *Digital Empires*'s argument for why the market-based model flounders. Bradford straightforwardly focuses on market externalities from social media and the internet-freedom agenda's loss of "credibility."[167] All such deficiencies can be resolved by more determined regulation. In contrast, Kokas points to a structural paradox of

---

[167] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 283–85.

free markets that are nested in a global competition with statist, authoritarian actors. The very dynamics that generate profit from data also weaken the state institutions supporting the deregulated market.

This dialectic—whereby internal contradictions of the free-market system tend to unravel the latter's preconditions—is a more powerful explanation for the waning influence of the market-based model than Bradford's reasoning. Kokas's dialectic also casts into doubt a meliorist embrace of the European rights-based model. As she acutely notes, the latter remains in thrall to the fundamental market precept of maximizing data collection, and hence remains vulnerable to exfiltration at scale by nondemocratic states.[168] In this light, Bradford's juxtaposition of market- and state-driven models looks inapt.

The logic of great-power conflict described in *Underground Empire* also complements, at least at a superficial level, *Digital Empires*'s prediction of a "bilateral digital world marked by continuing conflict."[169] Farrell and Newman, indeed, fill in an important gap in *Digital Empires*'s prediction on this score.[170] By tracing the ways in which Cold War infrastructures of communication and finance have already enabled U.S. hegemony, and by mapping the ways in which the United States leverages its asymmetrical power to shape other states' behavior, they identify a necessary precondition for the extension of geopolitical conflict to the digital realm: they show why states such as China, which have experienced rapid economic and military growth, might look for new ways to counter U.S. hegemony while they have the economic wind at their back.[171] As noted, U.S. military power is presently asymmetrically large,[172] such that even China's attempted extension of influence into the proximate South China Sea has been hotly contested. Bilateral tension is not a wind from nowhere: it arises from a structural logic of Cold War–era great-power competition that *Digital Empires*, rather oddly, leaves off the page.

---

168 KOKAS, *supra* note 8, at 20–21.

169 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 387.

170 *See supra* text accompanying note 103.

171 Professor Michael Beckley plausibly argues that rising states such as China are conscious that their window to act may be curtailed by flagging economic growth. Michael Beckley, *The Peril of Peaking Powers: Economic Slowdowns and Implications for China's Next Decade*, 48 INT'L SEC. 7, 9 (2023).

172 STEVENSON, *supra* note 98, at 2.

At the same time, *Underground Empire* makes Bradford's prediction of a growing convergence on a rights-based model seem puzzling and over-optimistic. Under conditions of increasing geopolitical stress, with a great-power opponent using a wide array of tactics to undermine democracies' ordinary operation, it seems unlikely that either the United States or Europe would gravitate toward a more rights-respecting position when it comes to the privacy and data-related interests of their own citizens. Surely, geopolitical strain induces more rebarbative, and less libertarian, policies. Governments will be more inclined to protect these prerogatives of their national champions, and so less inclined to rein in commercial practices that impinge on individual rights. Greater geopolitical stress tends to be correlated to less libertarian domestic policy. Bradford's panegyric to the possibility of "techno-democracies" coalescing to defend a somewhat inchoate idea of "liberal democracy" seems at odds with much historical experience.[173]

The top-line findings of *Trafficking Data* and *Underground Empire*, in short, have a complex and partly adversarial relation to Bradford's three-empire model. These tensions suggest that it would be profitable to examine more closely the latter's guiding assumptions and predictions, keeping in mind the more fulsome understanding of geopolitical conflict over digital regulation gleaned from all three books.

B. The Ideational Model of Nation-State Behavior Reconsidered

A central claim of *Digital Empires* is that the United States, China, and the EU are motivated by ideational differences. That is, nations embrace different models of digital regulation because they have "diverging economic theories, political ideologies, and cultural identities."[174] Bradford, to be clear, does not make the implausible claim that these ideologies explain any and all policy decisions. Rather, I think she is better understood to focus on the central tendencies of different regulatory models.[175]

In a sense, this chastening caution makes her claim both more plausible and also more elusive, and thus harder to evaluate. For any piece of countervailing evidence that undermines her

---

[173] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 388–91.

[174] *Id.* at 7.

[175] *See supra* text accompanying notes 46–50.

model, Bradford is open to conceding its existence and to fall back on an insistence about central tendencies that is harder to test or falsify. She would also be within her rights to insist that any challenge to her regulatory models fails without an alternative model being tendered.

Recognizing the force of these potential ripostes, I take two separate tacks in this and the next Section. In this Section, I put to one side states' rhetoric (which often will highlight ideas, even if they have no causal role)[176] and focus on policy actions. I then evaluate each of Bradford's three regulatory models in light of the whole body of evidence made available across all three books. Based on this broader evidentiary base, I suggest that her contrast between U.S. and European approaches to digital regulation is exaggerated. In effect, divergent rhetoric conceals a great deal of convergence. In contrast, I suggest that despite certain commonalities between the Chinese and U.S. models, her singling out of the state-driven model (when properly construed) as a distinctive approach to digital regulation is reasonable.

After addressing the force of Bradford's convergence hypothesis in Part II.C, I return in Part III to the "can't beat something with nothing" problem. That Part hence starts to sketch an alternative model for glossing states' geopolitical postures on digital regulation by looking at interests rather than ideologies as their determinants.

1. The free-market regulatory model reconsidered.

It is of course a platitude to observe that U.S. economic policy "rel[ies] on free markets and limiting regulatory intervention."[177] And like all platitudes, such anodyne pronouncements surely contain more than a grain of truth. But there is a substantial body of evidence that suggests such bromides offer no reliable guide to U.S. digital regulation.[178] Bradford focuses on speech regulation and antitrust.[179] Even accepting her comparative judgments about the weakness of U.S. state intervention in these domains, it is not at all clear that the U.S. "government stays out of the way."[180] But seeing why this is so requires adopting a broader lens

---

176 *See, e.g.*, BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 47–49 (describing the Clinton administration's various statements on internet freedom).

177 *Id.* at 38.

178 *See, e.g.*, FARRELL & NEWMAN, *supra* note 25, at 39.

179 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 42–47.

180 *Id.* at 38.

than Bradford's, one that makes room in particular for the insights of Farrell and Newman's *Underground Empire*.

Underground Empire offers evidence on this score because it provides a general framework for understanding the U.S. government's payoffs from intervention, and so mapping the extent of those efforts. As Farrell and Newman note, "Silicon Valley was an outgrowth of U.S. military spending."[181] Today's leading technology firms "emerge[d] from a relationship of dependency with the state's financial power."[182] In her excellent history, Professor Margaret O'Mara has documented how Silicon Valley technology firms' research and development has long been generously underwritten by the U.S. state.[183] Federal tax credits and procurement support, for example, helped Apple become a major industry player through its development and promotion of the iPhone.[184] As Professor Cecilia Rikap has shown, Microsoft, which has a substantial stake in OpenAI, persistently "rel[ies] extensively on the [public domain] work of scholars and public funding for its research," even as it uses intellectual property law to capture the profits from ensuing innovation.[185] In short, the U.S. government has simply not evinced a long-standing commitment to "an open, unregulated, and private sector-led digital economy" in all respects.[186] Just because the U.S. state has acted through subsidies, rather than regulation, does not mean that it has left the "free market" to its own devices.

This historical trend continues unabated. The federal government is now investing heavily in domestic manufacturing infrastructure to guarantee U.S. firms access to a secure supply of semiconductors—a critical resource in the digital domain.[187] As of 2023, some 90% of the most advanced chips in the world were

---

181 FARRELL & NEWMAN, *supra* note 25, at 39.

182 Marion Fourcade & Jeffrey Gordon, *Learning Like a State: Statecraft in the Digital Age*, 1 J.L. & POL. ECON. 78, 79 (2020).

183 The entanglement of California-based tech firms and government largesse is well told in MARGARET O'MARA, THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA 5 (2019) ("[P]ublic spending fueled an explosion of scientific and technical discovery, providing the foundation for generations of start-ups to come.").

184 MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE: DEBUNKING PUBLIC VS. PRIVATE SECTOR MYTHS 93–94 (2013).

185 Cecilia Rikap, *Capitalism as Usual?*, 139 NEW LEFT REV. 145, 156 (2023).

186 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 257.

187 *Id.* at 59–60 (discussing U.S. investments in technology in general terms); Antonio Andreoni & Simon Roberts, *Governing Digital Platform Power for Industrial Development: Toward an Entrepreneurial-Regulatory State*, 46 CAMBRIDGE J. ECON. 1431, 1445 (2022) (dating this resurgence in industrial policy to the 2008 financial crisis).

produced in just one country, Taiwan, and largely by just one company, TSMC.[188] Bipartisan administrations have used industrial policy to minimize the ensuing exposure to geopolitical risk. In 2020, TSMC announced a deal, brokered by the Trump White House, to build a fabrication plant in Arizona.[189] One of President Biden's signature legislative achievements, the 2022 CHIPS and Science Act,[190] extended this effort. According to the White House, the law authorized about $39 billion in manufacturing incentives.[191] This included $2 billion for legacy chips for automotive and defense systems. It also created a 25% investment federal tax credit for capital expenses for the manufacture of new semiconductors and related equipment.[192] The CHIPS Act thereby aimed to "accelerate development of advanced computing—from next-generation graphics processing units to high-density memory chips."[193] It was a recognition, explained Secretary of Commerce Gina Raimondo in February 2023, that "global competition" has become "increasingly about technology and chips, rather than just tanks and missiles"[194]—and the U.S. state cannot keep to the sidelines.

It is telling that when Bradford does take note of U.S. subsidies, she plays them down as "decentralized" and "true to [the United States'] market-driven instincts."[195] In my view, this is an inapt

---

188 *Taiwan's Dominance of the Chip Industry Makes It More Important*, THE ECONOMIST (Mar. 6, 2023), https://www.economist.com/special-report/2023/03/06/taiwans-dominance-of-the-chip-industry-makes-it-more-important.

189 Don Clark & Ana Swanson, *T.S.M.C. Is Set to Build a U.S. Chip Facility, a Win for Trump*, N.Y. TIMES (May 14, 2020), https://www.nytimes.com/2020/05/14/technology/trump-tsmc-us-chip-facility.html.

190 Pub. L. No. 117-167, 136 Stat. 1366 (codified in scattered sections of 2, 15, 26, 33, 40, 41, 42, 47, and 51 U.S.C.) (2022).

191 *FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China*, THE WHITE HOUSE (Aug. 9, 2022) https://perma.cc/N9W6-GMUM. As a consequence of the debt-ceiling conflict, Congress appropriated only 81% of these funds. Matt Hourihan, Mark Muro & Melissa Roberts Chapman, *The Bold Vision of the CHIPS and Science Act Isn't Getting the Funding It Needs*, BROOKINGS INST. (May 17, 2023), https://perma.cc/AT4T-FD2W.

192 *FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China*, *supra* note 191.

193 NAT'L AI RSCH. RES. TASK FORCE, STRENGTHENING AND DEMOCRATIZING THE U.S. ARTIFICIAL INTELLIGENCE INNOVATION ECOSYSTEM, at iv (2023).

194 *Remarks by U.S. Secretary of Commerce Gina Raimondo: The CHIPS Act and a Long-Term Vision for America's Technological Leadership*, U.S. DEP'T OF COM. (Feb. 23, 2023), https://perma.cc/KS7L-VU97.

195 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 58–59. Bradford also writes of the CHIPS and Science Act as the outcome of an international "subsidy race." *Id.* at 59. I think this is inapposite because it fails to take seriously the long history of U.S. subsidization of digital technologies by suggesting that the CHIPS Act is a response to a new, international phenomenon.

description of a pervasive and durable pattern of extensive funding for what can be characterized as de facto national champions.

The future pace of digital innovation in the United States, moreover, turns on an ongoing flow of government money. In recent decades, corporate laboratories have "receded in importance," with federally funded labs playing a growing role.[196] Since the 1970s, the federal government has funded research into new digital technologies through Industry-University Collaborative Research Centers, Engineering Research Centers, Materials Science and Engineering Centers, and the Small Business Innovation Research program.[197] Such largess, inevitably, breeds corporate dependence. As two leading AI researchers complained in 2020, the pace of domestic innovation can be undercut by "declining government investment in basic and foundational research."[198]

Such worries have not fallen on deaf ears. In 2023, the National Science Foundation expanded the number of "National AI Research Institutes" from eighteen to twenty-five.[199] These are intended to "catalyze collaborative efforts across institutions of higher education, federal agencies, industry, and others to pursue transformative AI advances that are ethical, trustworthy, responsible, and serve the public good," all while "promoting [ ] innovation" and "bolster[ing] America's AI R&D."[200] Of course, these measures complement large volumes of corporate expenditures on research. But it is significant that they are viewed as potentially dispositive in relation to international competitiveness.

In the absence of state intervention, by contrast, digital markets often are unsustainable. The United Kingdom, for example, recently announced plans to become a hub of AI innovation.[201] But only one company, Oracle, has a cluster of GPUs in the United Kingdom that use the leading GPU, Nvidia's A100 chip.[202] From

---

196 Fred Block, Matthew R. Keller & Marian Negoita, *Revisiting the Hidden Developmental State*, 52 POL. & SOC. 208, 214 (2024).

197 *Id.* at 215–16.

198 John Etchemendy & Fei-Fei Li, *National AI Research Resource: Ensuring the Continuation of American Innovation*, STAN. UNIV. HUMAN-CENTERED AI (Mar. 28, 2020), https://perma.cc/B5FY-MFKX.

199 *FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety*, THE WHITE HOUSE (May 4, 2023), https://perma.cc/SFM3-WFFV.

200 *Id.*

201 *How to Make Britain's AI Dreams Reality*, THE ECONOMIST (June 14, 2023), https://www.economist.com/britain/2023/06/14/how-to-make-britains-ai-dreams-reality.

202 *Id.*

this small resource base, it is effectively impossible for British companies to compete globally. Unwise industrial policy, in short, can thwart indigenous digital-market creation. The state and the market are inexorably entwined.

Given these patterns, it seems fair to express a concern that Bradford has been too selective in her account of the United States' free-market commitment. Many of her examples date from the period between the end of the Cold War and the global financial crisis of 2008,[203] ignoring what came before or what follows it. But this may be to mistake what the historian Professor Quinn Slobodian has acutely labeled a "brief early-millennial interregnum of hyper-globalisation when the [United States] opted for WTO cases rather than unilateralism" for evidence of "true" U.S. character.[204] *Digital Empires*, therefore, may reflect an impoverished partiality in respect to historical evidence of U.S. digital policy.

A more comprehensive view of the U.S. state's involvement in the digital marketplace also makes sense of the weaponized interdependence of digital infrastructure documented in *Underground Empire*. State investment in the private sector has payoffs because the resulting technologies "are becoming indispensable mediators of relations between the governing and the governed."[205] As Farrell and Newman show, the key role played by U.S. firms in global communications networks offers the United States unparalleled opportunities for shaping the incentives and choices of its geopolitical allies and opponents.[206] The "underground empire" may have been built with only a hazy understanding of geopolitical implications. Ordinary greed provides a quite sufficient explanation for its rise. But once it came into existence, the reliance of the U.S. state's extraterritorial reach on private actors became tolerably clear. What may be presented as the clockwork operation of the market mechanism's invisible hand in fact is probably better understood as just one more example of the U.S. state's capacity to leverage private firms and instruments for geopolitical ends.

More pointedly, the use of weaponized interdependence against Russia, Iran, and even Europe that is documented in

---

[203] *See, e.g.*, BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 266–68.

[204] Quinn Slobodian, *Nixon and the Art of Trade War*, THE NEW STATESMAN (May 17, 2024), https://perma.cc/V49G-CHLH.

[205] Marion Fourcade & Fleur Johns, *Loops, Ladders, and Links: The Recursivity of Social and Machine Learning*, 49 THEORY & SOC. 803, 813 (2020).

[206] FARRELL & NEWMAN, *supra* note 25, at 9, 31–60.

Underground Empire is hard to square with Bradford's claim that an ideological commitment to the free market best explains and predicts the United States' digital statecraft.[207] If she were correct about the centrality of ideological motives, then we would not expect to see increasing pressure to weaponize the supposedly neutral infrastructure of digital markets to noncommercial ends. Hence, it is not just that *Digital Empires* fails to canvas the conflicts documented in *Underground Empire*: the basic ideational model proposed in *Digital Empires* implies that those conflicts should rarely emerge. That they do suggests that interests matter more than ideas.

In skipping over these elements of U.S. statecraft, Bradford may well have erred by accepting too thin (and so tendentiously ideological) a concept of the free market. In this regard, *Digital Empires* often seems to take for granted that there is only one way of organizing a capitalist market, and this way demands that "the government . . . step aside to maximize the private sector's unfettered innovative zeal."[208] In truth, this categorical view is quite misleading. Since the middle of the twentieth century, the most ardent defenders of the free market have well understood that this zero-sum logic of market or state is false. They have argued for the creation of "apparatuses of juridical power to encase markets beyond democratic accountability" through a "turn to law."[209] Theoretical studies of market societies in the late twentieth century, moreover, have exploded the idea that there is only one way of using the state to enable a market society. In their canonical work on varieties of capitalism, Professors Peter Hall and Donald Soskice thus distinguished "liberal market economies, [where] firms coordinate their activities primarily via hierarchies and competitive market arrangements," from "coordinated market economies, [where] firms depend more heavily on non-market relationships to coordinate their endeavors."[210]

---

[207] *Id.* at 46–60, 159–61.

[208] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 33.

[209] QUINN SLOBODIAN, GLOBALISTS: THE END OF EMPIRE AND THE BIRTH OF NEOLIBERALISM 266 (2018); *id.* at 269 (noting that "a positive vision for the state is everywhere" in neoliberal theory); *see also* Richard Robison, *How to Build Market Societies: The Paradoxes of Neoliberal Revolution*, 10 NEW POL. ECON. 247, 247 (2005) (noting that "the rise of markets has often been accompanied by a dramatic centralisation and extension of state power").

[210] Peter A. Hall & David Soskice, *An Introduction to Varieties of Capitalism*, *in* VARIETIES OF CAPITALISM: THE INSTITUTIONAL FOUNDATIONS OF COMPARATIVE ADVANTAGE 1, 8 (Peter A. Hall & David Soskice eds., 2001) (emphasis omitted).

If free markets often coexist with a strong state, and if the nature of state–market relationships can vary dramatically across national contexts, then it may be that Bradford goes astray when she takes the absence of the state (or, indeed, any particular articulation of the state form) to index the comprehensive ideological triumph of free-market capitalism.

In sum, Bradford's treatment of the United States as following a market-driven model fails to account for vital and enduring forms of state intervention, glosses over important kinds of state power, and rests on a potent conceptual confusion about the relationship between the state and the market. It is thus far from clear that her market-driven regulatory model provides a perspicacious template of U.S. policymaking respecting digital regulation.

2. The rights-driven models reconsidered.

Just as the United States may talk in free-market terms, while pursuing interventionist policies, the EU is not quite as rights driven as *Digital Empires* suggests. Bradford's claim that "[f]undamental rights are deeply entrenched" in EU law rests mainly upon a recent series of European legislative initiatives relating to the digital economy.[211] These measures include the General Data Protection Regulation[212] (GDPR), the Digital Services Act[213] (DSA), the Digital Markets Act,[214] and the 2024 AI Act.[215] In particular, Bradford identifies the GDPR as a "gold standard" for privacy that is propagated via a Brussels Effect around the world.[216] Given the absence of national legislation in the United States protecting privacy or disciplining social media giants, these

---

211 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 110–23, 128–32. Bradford also relies on the EU's more vigorous enforcement of antitrust law as evidence that the EU "is geared at mitigating existing power asymmetries with the goal of cultivating a fairer digital economy." *Id.* at 124–26.

212 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

213 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

214 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

215 Artificial Intelligence Act, 2024 O.J. (L 1689).

216 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 112; *id.* at 335–36 (identifying emulation of the GDPR by other nations).

comprehensive, Europe-wide measures indeed seem at first blush powerful evidence of the distinctiveness of a rights-driven model extending from the Mediterranean to the Baltic.

Yet European law is simply not as sharply distinct from U.S. law as *Digital Empires* suggests. As a historical matter, most importantly, Bradford concedes that the liability protections of § 230 of the Communications Decency Act "largely resemble[ ]" shields for social media platforms in European law.[217] The DSA, to be sure, does diverge from U.S. law by imposing new legal constraints on harmful speech, targeted advertising, and dark designs.[218] But "open questions on enforcement and national-level implementation" mean that its effectual force remains much more uncertain than Bradford allows.[219] Regulation of large platforms may thus be more equivalent across the Atlantic than she suggests.

The absence of any dichotomous step change between a U.S. market-driven model and a European rights-driven one is also apparent in respect to privacy regulation. In addition to varying legislative regimes for privacy, Bradford highlights a series of high-profile conflicts over corporate data transfers from Europe to the United States.[220] The overall effect is to posit a contrast between (weak) U.S. privacy protections with (strong) European privacy law.

But this contrast is overdrawn. U.S. privacy law may be "piecemeal[,] . . . unpredictable[,] and difficult to understand."[221] Yet it is not the broad abrogation *Digital Empires* suggests. To begin, both "[t]he EU and the [United States] have roughly comparable constitutional and statutory mechanisms for the protection of privacy against unwarranted government surveillance."[222]

---

[217] *Id.* at 287. Unfortunately, Bradford stacks the rhetorical deck in favor of her conclusions on this point. On the one hand, discussion of § 230 of the Communications Decency Act foregrounds her treatment of the U.S. regulatory model. *Id.* at 43. But the observation that this measure has a parallel in European law is not presented in her parallel treatment of the EU's rights-driven model. It is offered as a throwaway caveat in her last substantive chapter. This does not seem to me an evenhanded way of engaging in comparative analysis.

[218] *Id.* at 120, 340, 381.

[219] *A Guide to the Digital Services Act, the EU's New Law to Rein In Big Tech*, ALGORITHM WATCH (Sept. 21, 2022), https://perma.cc/C3Z6-LJ96.

[220] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 229–31.

[221] Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, 18 COLO. TECH. L.J. 25, 37 (2020).

[222] David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT'L J. CONST. L. 220, 233 (2016); *see also* Peter Swire & DeBrae Kennedy-Mayo, *How Both the*

In respect to private actors, U.S. law is not silent. It opts instead for a different regulatory strategy from its transatlantic counterpart. Whereas European data protection law's "core focus [is] on principles of transparency and accountability," U.S. privacy law (primarily in the form of state tort law) trains "on stopping information from spreading."[223] To the extent there are gaps in U.S. data protection law, moreover, their practical significance appears to be minimized by "convergent regulatory styles [that] promote comparable best practices in data handling on both sides of the Atlantic."[224]

Even the "gold standard" GDPR has more ambiguous effects on privacy than *Digital Empires* allows. A 2021 study found that it reduced the amount of personal data regulated firms captured by about a tenth, but also make it easier to identify and track those whose data was still obtained.[225] National regulators also "struggl[e]" to enforce the GDPR, while European complaint mechanisms have been "bloated and slow[ ] down enforcement."[226] As a result, five years after the GDPR entered into force, some 85% of complaints filed before national authorities had not been decided, some having languished for years.[227] A similar concern

---

EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information, 66 EMORY L.J. 617, 636 (2017) (identifying a series of "plus factors" or "ways in which U.S. privacy protections reasonably can be considered at least as strict or stricter than EU privacy protections").

[223] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. REV. 93, 101 (2020) ("Data protection arguably has a different scope than privacy—in some ways broader and in some ways narrower.").

[224] William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 988 (2016). Moreover, a full accounting of U.S. privacy would need to account for the way that "[s]tate attorneys general have been nimble privacy enforcement pioneers." Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 750 (2016). *Digital Empires* is silent on substate actors—which is a serious gap in the privacy context.

[225] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Effect of Privacy Regulation on the Data Industry: Empirical Evidence from GDPR*, *in* EC '21: PROCEEDINGS OF THE 22ND ACM CONFERENCE ON ECONOMICS AND COMPUTATION 93, 93 (2021). Another study found that the GDPR did not increase trust in data collectors. *See* Paul C. Bauer, Frederic Gerdon, Florian Keusch, Frauke Kreuter & David Vannette, *Did the GDPR Increase Trust in Data Collectors? Evidence from Observational and Experimental Data*, 25 INFO., COMM. & SOC'Y 2101, 2101 (2022).

[226] Matt Burgess, *How GDPR Is Failing*, WIRED (May 23, 2022), https://www.wired.com/story/gdpr-2022.

[227] *5 Years of the GDPR: National Authorities Let Down European Legislator*, NOYB (May 23, 2023), https://perma.cc/4RWP-QCEZ. More recent enforcement actions suggest a still murky picture. In January 2023, the Irish data protection authority levied a large fine against Meta under the GDPR. Vincent Manancourt, *€390M Fine Strikes Blow to*

arises respecting the new AI Act. According to Professors Nathalie Smuha and Karen Yeung, the AI Act relies upon companies to make their judgments about the risks presented by different AI systems, or else leans on industry-dominated standard-setting organizations.[228] They are, reasonably enough, skeptical that profit-oriented firms will rush to subject their profits to demanding regulatory standards.[229]

Although Bradford notes briefly some shortcomings in European enforcement,[230] *Digital Empires*'s central focus on the text of statutes, rather than on their enforcement, leads to conclusions about the efficacy of the GDPR and other European laws that are in some tension with observed patterns of (non)enforcement.

None of this is to say that U.S. and European privacy law move entirely in lockstep, share philosophical premises, or have parallel effects. As *Digital Empires* observes, they diverge in certain ways. But these variances are differences of emphasis, not kind. They do not justify Bradford's categorical distinction between one jurisdiction that generally genuflects to rights and another that disparages them.

Another implication of the distinction between the U.S. market-driven model and European rights-driven model is that the EU's leaders are not committed to free markets in the same way as U.S. policymakers. Again, the contrast is overdrawn. Bradford understates the extent to which European law, like U.S. law, reflects a profound and long-standing commitment to markets as such. To be sure, she does in passing recognize that EU regulation has a "dual objective" of advancing rights and also building a "single market," and that the EU has a "neoliberal foundation."[231] But this fleeting reference does not do justice to

---

Meta's Ad-Fueled Business Model, POLITICO (Jan. 4, 2023), https://perma.cc/XM2Y-TAFP. Two months later, Meta announced that it was switching its legal basis for the processing of personal data, so extending the legal dispute. Sam Schechner & Jeff Horwitz, *Meta to Let Users Opt Out of Some Targeted Ads, but Only in Europe*, WALL ST. J. (Mar. 30, 2023), https://www.wsj.com/article/meta-to-let-users-opt-out-of-some-targeted-ads-but-only-in-europe-44b20b6d. For a more optimistic take on the GDPR, see Morgan Meaker, *The Slow Death of Surveillance Capitalism Has Begun*, WIRED (Jan. 5, 2023), https://www.wired.com/story/meta-surveillance-capitalism.

[228] Nathalie A. Smuha & Karen Yeung, *The European Union's AI Act: Beyond Motherhood and Apple Pie?*, *in* THE CAMBRIDGE HANDBOOK OF THE LAW, ETHICS AND POLICY OF ARTIFICIAL INTELLIGENCE 16, 24 (Nathalie A. Smuha ed., 2025); BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 139–40, 376.

[229] Smuha & Yeung, *supra* note 228, at 29–30.

[230] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 376–78.

[231] *Id.* at 130–32.

the profoundly market-enabling, even neoliberal, character of the European project.

The present network of Europe-wide institutions began to emerge in the 1950s as a result of the economic and geopolitical pressures of postwar Europe grappling with the geopolitical implications of Germany's rebirth.[232] *Digital Empires* picks out one regulatory strand of the pan-European activity that followed. But it ignores other, arguably far more central, legal planks of the European project. Since the 1951 and 1957 treaties that initiated European integration, economic integration has been central; early treaties were silent as to individual rights.[233] The ensuing series of basic treaties have centered on the idea of "market solidarity," which has even been characterized as being "written into the EU's genetic code."[234] And the resulting process of integration has often involved a mandate of "mainstream neoliberal policies" that "circumvent and erode" national traditions of social democracy.[235] In no domain is this more evident than in the core European project of a single currency. The eurozone's monetary architecture for a single currency has been fairly described as a "joint decision trap in an inter-state federation" that "generates a quintessentially neoliberal outcome as the threshold for reaching a positive decision is beyond the actors concerned."[236] European monetary union presupposes an "uncompromising commitment to free movement of capital" that has led to an "entrenchment of the neoliberal policy agenda in the EU constitutional order" enforced

---

232 Craig Parsons, *Showing Ideas as Causes: The Origins of the European Union*, 56 INT'L ORG. 47, 54 (2002) (summarizing process and historical debates).

233 J.H.H. Weiler, *The Transformation of Europe*, 100 YALE L.J. 2403, 2417 (1991) (explaining that only starting in 1969 did the European Court of Justice "assert[ ] that it would, nonetheless, review Community measures for any violation of fundamental human rights").

234 Gareth Dale & Nadine El-Enany, *The Limits of Social Europe: EU Law and the Ordoliberal Agenda*, 14 GERMAN L.J. 613, 613 (2013).

235 Christoph Hermann, *Neoliberalism in the European Union*, 79 STUD. POL. ECON. 61, 61 (2007).

236 J. Magnus Ryner, *Is European Monetary Integration Structurally Neoliberal? The Origins of the EMS and the 1977–1978 Locomotive Conflict*, 20 COMP. EUR. POL. 731, 736–37 (2022). For an account that distinguishes France's initial aim in monetary integration of "increas[ing] the capacity of the state to meet the expectations of its citizens," see Helen Thompson, *The Nation-State and International Capital Flows in Historical Perspective*, 32 GOV'T & OPPOSITION 84, 110 (1997). For a useful account of the emergence of the Euro as "a policy of fiscal consolidation in the transition to neoliberal, financialized economies," see Wolfgang Streeck, *Why the Euro Divides Europe*, 95 NEW LEFT REV. 5, 16–17 (2015).

by the European Central Bank.[237] In moments of crisis, the Bank has acted consistent with this ideology and has used its role as lender of last resort to force market-liberalization measures on recalcitrant debtor nations.[238]

Bradford's claim that the European project aims at "mitigating existing power asymmetries,"[239] in short, rests on a highly selective treatment of EU law. It focuses on a handful of regulatory initiatives of recent vintage and uncertain on-the-ground effect. It also ignores the profound and extensive changes wrought by neoliberal economic choices tightly woven into the European treaty lattice since the 1950s. While her observations about the GDPR, the DSA, and the AI Act are all well-taken in isolation, it seems to me that an accurate and fair-minded evaluation of the European legal project that does not center these historically rooted elements of European policymaking obscures more than it reveals.

A more balanced accounting of European policymaking through law, with respect to markets, individual dignity, and privacy rights, suggests a far more complex story. One way of telling that tale, associated with the historian Professor Samuel Moyn, takes rights as "unambitious in theory and ineffectual in practice" and "merely nipping at the heels of the neoliberal giant."[240] But one does not need to go as far as Moyn in his acid cynicism about all human rights talk to see that *Digital Empires*'s celebration of Europe's "human-centric and rights-driven approach"[241] calls out for some caveats and qualifying provisos.

3. The state-driven model affirmed.

The state-driven regulatory model is defined alternatively in terms of either purposes or means in *Digital Empires*. In my view, it is sensibly glossed largely in terms of means. As to ends, China's government is said to deploy new digital technology to "fuel the country's economic growth . . . while maintaining social

---

[237] Marco Dani, *Openness, Purposiveness, and the Realignment of the EU and the Democratic and Social Constitutional State*, 24 GERMAN L.J. 1099, 1116–18 (2023). On the enforcement role of the Bank, see WOLFGANG STREECK, HOW WILL CAPITALISM END? ESSAYS ON A FAILING SYSTEM 162 (2016).

[238] Andy Storey, *Authoritarian Neoliberalism in Europe: The Red Herring of Ordoliberalism*, 45 CRIT. SOCIO. 1035, 1040 (2019) (offering Cypriot and Greek case studies).

[239] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 124.

[240] SAMUEL MOYN, NOT ENOUGH: HUMAN RIGHTS IN AN UNEQUAL WORLD 216 (2018).

[241] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 105.

harmony and control over its citizens' communications."[242] With the exception of the last phrase of that formulation, this is a claim that can plausibly be made of almost any nation-state. Hence, the Chinese state-driven model is not distinguished by a unique state-centered purpose.

As to means, Bradford identifies the restriction of domestic markets, internet censorship, and broad surveillance of the population as characteristic of the Chinese model.[243] I think *Digital Empires* is reasonably read as centering the frequent use of these digital policy instruments *for the purpose of political control* as the distinctive characteristic of the state-driven model.[244]

Read in this way, the state-driven regulatory model is the most persuasive of the three ideational regulatory types that *Digital Empires* develops. This is not because other sovereigns have any dearth of digital surveillance power. As Farrell and Newman point out, one source of U.S. hegemonic power is its control of key nodes of the global telecommunications infrastructure, with all of the access to personal data that entails.[245] While Kokas focuses on the way that the commercial creation and exploitation of data empowers the Chinese state, a parallel point can be made about the U.S. state. The NSA, for example, purchases the internet browsing history of those within the United States from data brokers.[246] (This is yet another example of why "the market" and the "the state" do not stand in opposition to each other: they can be mutually empowering instead.) Further, the United States, like China, has accumulated a wide array of digital surveillance tools, including "computerized language translation, biometrics and facial recognition technology, machine learning to detect anomalies and patterns, information fusion . . . , and social network analysis" as an "ordinary part" of government.[247]

---

[242] *Id.* at 69; *id.* at 72 (describing China's goals as "economic growth and geopolitical prominence").

[243] *Id.* at 76–91.

[244] It would be implausible to define that regulatory model by the purpose of strengthening the state as such, and I take Bradford to be making a more sophisticated claim.

[245] FARRELL & NEWMAN, *supra* note 25, at 9, 31–60.

[246] Charlie Savage, *N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says*, N.Y. TIMES (Jan. 25, 2024), https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html; Kevin Collier, *U.S. Government Buys Data on Americans with Little Oversight, Report Finds*, NBC NEWS (June 13, 2023), https://www.nbcnews.com/tech/security/us-government-buys-data-americans-little-oversight-report-finds-rcna89035.

[247] BYRON TAU, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE 28 (2024). Oddly,

On the other hand, the manner and frequency with which such instruments are used by the Chinese state in respect to its whole population for the purpose of political control seems to me distinctive and different from the U.S. and the European cases (at least for now).[248]

Consistent with Bradford's ideational theory, the deployment of state resources for population-level political control by Chinese governments long predated the digital age. The various digital instruments of surveillance and control, therefore, slotted into a well-defined and well-understood institutional setting that has long been oriented toward political control on the party-state's behalf.

In an illuminating recent treatment of the Chinese "sentinel state," Professor Minxin Pei described the way in which new digital technologies have been layered on top of not just the "Leninist party-state" but also the imperial baojia system, which "combined elements of urban planning, census taking, tax collection, and law enforcement to enforce social order."[249] Even before digital surveillance tools were widely available, the Chinese party-state had some 3.5 of every 1,000 of its population under surveillance.[250] With this history in mind, Pei argues that digital repression at scale is feasible only in China because it has built on an army of extant "security bureaucracies that are generously funded, well-organized, and carefully designed to deter and contain political threats to the party-state."[251] Pei's work offers rich confirmatory evidence of Bradford's argument for the importance

---

Bradford discusses Western companies' export of digital technologies of political control, *see* BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 316, but says little about the domestic use of such tools.

248 Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html; *see also* Paul Mozur, *Looking Through the Eyes of China's Surveillance State*, N.Y. TIMES (July 16, 2018), https://www.nytimes.com/2018/07/16/technology/china-surveillance-state.html. An algorithmic classification tool winnows surveillance data for ethnic Uyghur faces, producing a detailed accounting of the precise movements and actions of a single ethnic class. *See* Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; *see also* Steven Feldstein, *The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression*, 30 J. DEMOCRACY 40, 44 (2019) (documenting how tracking software is embedded in platforms such as WeChat, so the state is immediately aware if crowds form).

249 MINXIN PEI, THE SENTINEL STATE: SURVEILLANCE AND THE SURVIVAL OF DICTATORSHIP IN CHINA 20–21 (2024).

250 *Id.* at 164–71 (describing the Key Populations program as it operated between the 1990s and 2010s).

251 *Id.* at 3, 23–24 (describing security bureaucracy in China).

of historically hegemonic regulatory models for shaping digital policy in their national settings. Once the state is oriented in a particular way, that is, it will tend to find ways to use new affordances consistent with its habituated understandings of means and ends.

At the same time, Bradford may overstate the extent to which a sentinel-state mentality shapes digital policymaking in China. For instance, Bradford expresses skepticism about the motives for the party-state's increasingly tight regulation of tech companies.[252] Addressing "public concerns about inequality or exploitative business practices is unlikely to be [its] sole motivation."[253] But this may be off the mark, depending on how much weight the word "sole" is meant to carry.

In a recent, deeply researched study of Chinese privacy law, Professor Mark Jia has argued that the "central purpose of" those measures "is to enhance the party-state's legitimacy by co-opting privacy and framing the party-state as privacy's primary protector," and thereby to diffuse "significant social discontent over data abuse."[254] Mitigating public discontent is, of course, in the rational self-interest of an authoritarian leader as well as of a reelection-hungry democratic leader.[255] While authoritarian leaders are responsive as a result of nondemocratic mechanisms, the basic finding of Jia's work—that China's party-state is responding to pressures seeded by popular preferences—suggests that its privacy law should not be understood as exclusively "state-driven" in its effects and its ends in the way that Bradford suggests.[256]

4. Reevaluating ideational approaches to digital regulation.

Digital Empires's tripartite ideational typology of national digital regulatory models is a partial success. On the one hand, it overstates the differences between the U.S. and the European models. On the other hand, it persuasively singles out a distinctive Chinese approach. At a minimum, it leaves open the question whether an ideational template best explains divergent

---

252 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 96.

253 *Id.*

254 Mark Jia, *Authoritarian Privacy*, 91 U. CHI. L. REV. 733, 764 (2024) [hereinafter Jia, *Authoritarian Privacy*].

255 *Id.* at 808; *see also* Jidong Chen, Jennifer Pan & Yiqing Xu, *Sources of Authoritarian Responsiveness: A Field Experiment in China*, 60 AM. J. POL. SCI. 383, 383 (2016) ("A growing body of research suggests that authoritarian regimes are responsive to societal actors.").

256 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 69.

approaches to digital regulation. Ideologies of regulation certainly do some explanatory work, especially when they reflect long-standing patterns of state organization (as in China). But the ideas of "market-driven" and "rights-driven" models in particular are so baggy, so capacious, and so capable of flexible redefinition that it is a mistake, I think, to conclude that they offer that much by way of causal explanation. In this light, the more precisely gauged, empirically grounded arguments of *Trafficking Data* and *Underground Empire* gain a certain luster.

This closer examination also casts light on a key, albeit implicit, premise of Bradford's typology. The latter assumed that the market-driven, rights-driven, and state-driven models are distinct ideals, even though in practice states dabble in the use of different tools, drawing elements from different models. It is not at all clear that a state ideologically committed to extensive free markets needs to abandon rights, even if the commitment to markets might constrain the kinds of rights it can plausibly recognize. Similarly, the example of Chinese privacy laws suggests that a single policy choice can simultaneously advance both statist and rights-related goals. The three regulatory models, in short, seem on closer consideration to be more complementary rather than mutually exclusive.

C. The End State of Global Conflict over Digital Commerce

The three-empire model of *Digital Empires* yields two main predictions. One is probably right, albeit for reasons that have little to do with Bradford's underlying model of competition between regulatory models. The second is more questionable. It raises a host of difficult questions about the geopolitical dynamics of digital regulation.

The first prediction is "continuing conflict" between the United States, perhaps alongside other democracies, and China.[257] Recall that *Digital Empires* offers no explanation for why that conflict emerges or intensifies.[258] *Trafficking Data* and *Underground Empire* help fill the gap. Both identify structural asymmetries between the United States and China in data markets and global infrastructure control, respectively, that operate as fault lines: when one sovereign power exploits their advantages, they generate opposition and resistance from other

---

[257] *Id.* at 386–93; *see also supra* text accompanying notes 57–59.

[258] *See supra* text accompanying note 83.

sovereigns. These frictions, to be sure, are but fragments of a larger historical story. They emerge in a context of wider, tectonic shifts in the relations of major global powers that are increasingly carrying nation-states toward geopolitical conflict.[259] Predictions of U.S.–China conflict rest on a firm geopolitical logic that does not need to appeal to digital regulatory dynamics. They are a function of the enduring material legacies of Cold War conflicts and the later frictions between a dominant and a rising potential hegemon.

Bradford's second prediction is more interesting. It departs from the conventional wisdom: it anticipates the convergence of "democratic countries" on the EU's "rights-driven" model.[260] How the "rules and norms that govern the digital economy" are set, she asserts, is a "significant" question.[261]

Recall that her conclusion that the EU's rights-driven model is winning this contest in fact blends two slightly distinct claims, and that this is one of the central ambiguities of her account.[262] On the one hand, there is a claim that the EU's specific regulatory choices will increasingly be adopted by other jurisdictions in a digital version of the Brussels Effect.[263] On the other hand, there is a claim that the United States will abandon its laissez-faire approach and adopt its own regulation.[264] The first claim concerns the regulatory dominance of a specific jurisdiction; the second concerns the hegemony of a particular idea about how to regulate (i.e., to advance rights rather than markets). It is a hegemony whose appeal rests on its putative ability to find a middle path between the alleged extremes of the state-driven and the market-driven models. In thinking about this prediction, I will try to be clear about which of these two strands I am addressing at any given point.

As a threshold matter, I want to recognize that this second version of Bradford's prediction holds a kernel of truth. Bradford is

---

259 For a powerful account of why changes in the "liberal international order" caused "the rise of China, . . . along with the revival of Russian power," see John J. Mearsheimer, *Bound to Fail: The Rise and Fall of the Liberal International Order*, 43 INT'L SEC. 7, 7–8 (2019); *accord* Graham Allison, *The Thucydides Trap*, 9 FOREIGN POL'Y 73 (2017) (exploring strategic dynamics of the shift from a unipolar to a multipolar world).

260 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 361–63; *see supra* text accompanying notes 60–63.

261 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 361.

262 *See supra* text accompanying notes 80–84.

263 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 324–36.

264 *Id.* at 351 ("[E]ven the [United States] may now be inching toward the European rights-driven approach.").

quite right to observe that market inelasticities, economies of scale, and first-mover advantages make the GDPR, the DSA, the AI Act, and their ilk attractive standards for multinational standards and for some other jurisdictions seeking to reduce their compliance and enactment costs, respectively.[265] She is also right to observe that some global tech firms have sometimes adopted European standards across their global systems so that non-Europeans benefit de facto from the rights created by European law.[266] And she justly observes that European demands for adequate data protections in countries receiving European data have pushed other countries to strengthen privacy laws, while the GDPR itself has "inspired" regulation in other countries—just as the AI Act served as a model for Colorado's AI regulation.[267] Even though *Digital Empires* overstates the extent to which nation-states must choose between the market-driven and the rights-driven models, and even though the relation of the market and the state can take manifold shapes,[268] Bradford is persuasive in identifying one vector of geopolitical influence.

But I am less confident in her conclusion that this is a "significant" vector that will have a profound effect on the terms of global digital regulation.[269] My worries on this score rest on several, somewhat distinct grounds.

First, Bradford's argument for the delegitimation of the market-driven model rests mainly on evidence of growing distrust of firms such as Meta and Alphabet as a result of various scandals.[270] But it is not clear that such distrust offers a new and independent motive for greater regulation. For one thing, neither Facebook nor Google is experiencing declines in market share in non-U.S. jurisdictions.[271] This fact seems in tension with

---

265 BRADFORD, BRUSSELS EFFECT, *supra* note 21, at 25–65.

266 *See, e.g.*, *id.* at 1330–31 (noting the positive spillovers of the GDPR's "privacy by design" mandates).

267 *See supra* text accompanying notes 3–6. For a careful analysis of the AI Act's extraterritorial spillovers, see CHARLOTTE SIEGMANN & MARKUS ANDERLJUNG, CTR. FOR THE GOVERNANCE OF AI, THE BRUSSELS EFFECT AND ARTIFICIAL INTELLIGENCE: HOW EU REGULATION WILL IMPACT THE GLOBAL AI MARKET 22–23 (2022) (noting the possibility of a "de facto" Brussels Effect for some parts of the AI Act but finding it "difficult to assess the likelihood of a de jure effect").

268 *See supra* Part II.B.4.

269 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 28.

270 *Id.* at 379–84.

271 Stacy Jo Dixon, *Facebook Daily Active Users (DAU) in Europe from 4th Quarter 2012 to 4th Quarter 2023*, STATISTA (Apr. 26, 2024), https://perma.cc/T3ND-YSKQ; *Search Engine Market Share Europe: July 2023–July 2024*, STATCOUNTER, https://perma.cc/VQH8-L9L6.

Bradford's claims about dramatic *falls* in public trust, which seem (on her view) to be a predicate of greater regulation.

Moreover, it is hardly clear that European states (or consumers) deeply trusted U.S. tech firms in the first place. To the contrary, other nation-states have long had more than enough reason to distrust, and hence to seek to regulate, U.S. firms. European governments, for instance, look to the French company Mistral AI to "propel the region into a high-stakes match with the United States and China."[272] China has an extensive domestic ecosystem of "research talent, data, and corporate investment" that, by some measures, rivals the United States'.[273]

Even within the United States, the evidence of a recent turn against regulation is far from robust. In May 2024, for example, a bipartisan Senate working group released a "roadmap" for AI policy in the United States.[274] Its title stressed "innovation," and at its heart was a call for "at least $32 billion per year for (non-defense) AI innovation."[275] A large measure of this new funding would inevitably flow to the firms with AI capacity—i.e., the very firms that Bradford describes as having lost the government's trust are gaining increasing access to its purse. The underlying causal mechanism of *Digital Empires*'s convergence prediction, in short, is both theoretically and empirically underpowered.

Second, it is not clear that regulatory spillovers are indeed as significant as *Digital Empires* asserts in either scope or effect. Consider first the question of scope. Regulatory spillovers from Europe are most likely in "less geopolitically powerful jurisdictions" with "less regulatory capacity and international bargaining power."[276] Yet, by and large Bradford ignores these jurisdictions.[277] By her own reckoning, these effects are not plainly consequential in geopolitical terms.

Further, there is good reason to doubt spillovers to other major metropolitan markets. Technical advances may be making it

---

[272] Liz Alderman & Adam Satariano, *Europe's A.I. 'Champion' Sets Sights on Tech Giants in U.S.*, N.Y. TIMES (Apr. 18, 2024), https://www.nytimes.com/2024/04/12/business/artificial-intelligence-mistral-france-europe.html.

[273] Mariano-Florentino Cuéllar & Matt Sheehan, *AI Is Winning the AI Race*, FOREIGN POL'Y (June 19, 2023), https://foreignpolicy.com/2023/06/19/us-china-ai-race-regulation-artificial-intelligence.

[274] BIPARTISAN SENATE AI WORKING GRP., DRIVING U.S. INNOVATION IN ARTIFICIAL INTELLIGENCE 4 (2024).

[275] *Id.* at 5.

[276] SIEGMANN & ANDERLJUNG, *supra* note 267, at 24.

[277] *See supra* text accompanying notes 68–79.

easier for companies to partition products by geography, offering different versions of a good that align with different nation-states' preferences. Such geolocational tools now "permeate internet operations."[278] So in jurisdictions with distinctive regulatory preferences, such as China, many firms "already have differentiated products."[279]

In addition, to the extent that regulatory spillovers are important, *Digital Empires* skips over an obvious and important question: Given the size of the Chinese consumer market, why would we not expect a "Beijing Effect" to dominate in practice over any Brussels Effect? China, after all, is "the world's largest trading power and its second-largest economy,"[280] producing some 35% of the world's manufactured goods.[281] Europe is arguably no less in thrall than countries that are part of the Belt and Road Initiative. In 2023, German companies invested some $11 billion in China.[282] Given such large dependency on Chinese markets, it might seem likely that Chinese regulatory norms are likely to diffuse more rapidly than European ones as producers adapt to the Chinese market.[283] Indeed, the extent of Chinese influence is evident in the lukewarm European response to U.S. calls for a ban on Huawei 5G equipment. As Farrell and Newman explain, the U.S. government has "engaged in an unprecedented campaign" to limit Huawei's global reach.[284] Yet only ten European countries had prohibited the

---

[278] Jack Goldsmith & Eugene Volokh, *State Regulation of Online Behavior: The Dormant Commerce Clause and Geolocation*, 101 TEX. L. REV. 1083, 1104 (2023); *see also* Marketa Trimble, *Introduction to Geo-Blocking*, *in* THE EU GEO-BLOCKING REGULATION 1, 2–3 (M. Trimble ed., 2024) (explaining that "'geo-blocking' refers to the practice of restricting access to Internet content based on the physical location of the user who attempts to access the content").

[279] SIEGMANN & ANDERLJUNG, *supra* note 267, at 24.

[280] Matt Ferchen & Mikael Mattlin, *Five Modes of China's Economic Influence: Rethinking Chinese Economic Statecraft*, 36 PAC. REV. 978, 998 (2023); FARRELL & NEWMAN, *supra* note 25, at 108 (explaining how China has wielded "market access" as a geopolitical cudgel).

[281] Damien Cave, *In China's Backyard, America Has Become a Humbler Superpower*, N.Y. TIMES (June 13, 2024), https://www.nytimes.com/2024/06/13/world/australia/us-changing-role-asia-pacific.html.

[282] Melissa Eddy, *Why Germany Can't Break Up with China*, N.Y. TIMES (Apr. 16, 2024), https://www.nytimes.com/2024/04/16/business/germany-china-tariffs.html.

[283] It may be that Chinese firms play different roles in the supply chain for digital goods than, say, Korean or Taiwanese firms, and as such have fewer opportunities to insist on their standards. Of course, the dynamic nature of supply chain development makes any such limitation a contingent and perhaps fleeting one.

[284] FARRELL & NEWMAN, *supra* note 25, at 80.

company as of February 2024.[285] In this context, Kokas's reluctance to lean on European-style regulation as a panacea against data exfiltration to China seems quite sensible: European dependency on Chinese markets undercuts the incentive to create or enforce robust legal protections against that phenomenon.

Now consider the effects of regulatory spillover: When China adopts certain terms in its data privacy law that echo the GDPR's terms,[286] does this suggest that the EU has exercised a meaningful form of influence? *Digital Empires* offers little conclusive evidence of actual emulation. And as Bradford rightly observes, the Chinese data privacy law tracks its European antecedent only so far as doing so serves the party-state's purposes.[287] The Chinese party-state is thus able to advance a rights-driven vision in certain respects, while also pursuing its state-focused ambition in other ways. Again, what *Digital Empires* presents as mutually exclusive regulatory models turn out, in practice, to be highly permeable, potentially overlapping, and even complementary state projects.

The effect is, on one level, banal: regulatory diffusion across nations occurs across many different policy areas.[288] At another level, its implications are trivial, for it is not at all clear that it indexes a significant form of transnational power. After all, the EU does not plainly benefit either directly or indirectly if another jurisdiction free rides on the legislative effort that went into creating a new regulation.[289] Such free riding can be styled as "influence." Or it might just be another way of being a patsy.

Third, it would have been useful for Bradford to consider the possibility of conflict between regulatory spillovers and other vectors of geopolitical influence. The assertion that the former are meaningful in scale depends in important part on whether other jurisdictions have alternate, nondigital tools to resist or undermine these effects. In the main, the European regulation that is the focus of her thesis targets companies and private actors, imposing obligations on their conduct directly. But, as Kokas, Farrell, and Newman underscore, there are other ways of

---

[285] Cynthia Kroet, *Most EU Members Not Implementing Huawei, ZTE 5G Ban, Data Shows*, EURONEWS (Feb. 12, 2024), https://perma.cc/US9D-ZTXV.

[286] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 334; *accord* Jia, *Authoritarian Privacy*, *supra* note 254, at 750–53.

[287] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 334–35.

[288] Katerina Linos, *Diffusion Through Democracy*, 55 AM. J. POL. SCI. 678, 679 (2011).

[289] To the contrary, the ordinary inference is that the inability to capture the value of positive spillovers is correlated with insufficient incentives to engage in an activity.

wielding extraterritorial influence that do not target the primary conduct of firms.

For example, imagine that a small nation-state faces a choice between a European data privacy rule and Chinese subsidies flowing through its Digital Silk Road program. How likely is it that this hypothetical nation will eschew money in favor of more rights-respecting regulation? Or imagine that China's investments in international standard-setting authorities pay off, and Chinese technical standards are adopted for critical pieces of telecommunications infrastructure.[290] To what extent does a Brussels Effect with respect to privacy or AI regulation persist, given that reshaping of basic technological terms in ways that might enable en masse data exfiltration? Would it matter much in practice if China has already set the basic terms of the technology's use? I suspect that the answer to these questions will vary from case to case. But it also seems to me imprudent to assume that regulatory spillovers can always, or even often, be meaningful in the face of other forms of countervailing power.

In the end, I am unpersuaded by the stronger version of *Digital Empires*'s convergence prediction. I think Bradford is correct to flag a number of regulatory spillovers from EU lawmaking efforts for digital technologies. But as a matter of her own theoretical typology, it is hard to make much of this fact. After all, her distinct regulatory models are capable of coexistence, to some extent, within the same jurisdiction.

To the extent that there is some digital regulatory diffusion, moreover, this neither reflects nor changes the balance of geopolitical power between two nations. There is also reason to think that the movement of regulatory innovations can be blocked or undercut by other vectors of state influence, including infrastructural power of sorts.

The net result is not so much a repudiation of a digital Brussels Effect—but more simply a puzzle. What, if any, are the geopolitical stakes of that phenomenon? If everyone agreed with Brussels when it came to regulatory strategy anyway, would it really matter?

---

[290] BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 302–08; *see also* Aziz Huq, *A World Divided over Artificial Intelligence*, FOREIGN AFFS. (Mar. 11, 2024), https://www.foreignaffairs.com/united-states/world-divided-over-artificial-intelligence (documenting more recent standard-related developments).

III. REIMAGINING THE GEOPOLITICS OF DIGITAL REGULATION

I have so far pressed on what I think are weaknesses in the overall typology offered by *Digital Empires*, drawing on the contributions of *Trafficking Data* and *Underground Empire* to add heft to those critiques. I do not, however, want to suggest that the general framework for thinking about the geopolitics of digital regulation drawn up in *Digital Empires* is unimportant. To the contrary, while I have disagreed with some of its particulars, I nonetheless adjudge it an ambitious and valuable contribution—the first sustained, intellectually serious effort at a comprehensive depiction of a significant domain of global regulation.

In this Part, I build on that typology, drawing more broadly upon the insights of all three books under consideration here in order to start sketching an alternative general framework for thinking about the geopolitics of digital regulation that corrects for some of its limits.

Concededly, the effort that follows is far thinner than Bradford's impressively detailed treatment (as it must be, given the form and limits of a review of this sort). My aim is not to displace her work but to show how one might build constructively upon it to fashion a more perspicacious model to the same effect. What follows can thus be glossed as a series of friendly amendments.

To my mind, the challenge of conceptualizing the geopolitics of digital regulation is twofold. A first challenge turns on how the motives of nation-states or their ilk[291] are characterized. In Part II, I offered some reasons for thinking that an exclusively ideational typology falls short, albeit without entirely rejecting the influence of ideology. The challenge is hence how to integrate ideational with material interests, which I flagged above,[292] and the institutional matrices of domestic politics by which these are translated into policy. A second challenge turns on how to nest various forms of contestation over digital regulation in relation to each other, and also to other vectors of geopolitical conflict, given the possibility of their coexistence.

Answering these challenges, I would propose at a first approximation that states in this context should be understood to pursue the interests of a dominant technopolitical elite, albeit

---

[291] In the balance of this Part, I will omit this caveat and simply use the term "nation-states" or refer to the relevant participants in geopolitical competition, including the EU.

[292] *See supra* text accompanying notes 98–102.

under constraints created by military, economic, and material forms of geopolitical conflict.

Digital regulation, on this view, is a distinctly second-order species of international conflict. Generally, it will be subordinated to those other forms of conflict (including conflict over technical infrastructure, data, or other primary resources). At times, this means that digital regulation will be determined by the overall balance of political forces between nation-states; at other moments, the ancillary rank of digital regulation will mean that non-great powers have a degree of freedom to fashion policy as they will. On this account, European regulatory spillovers may be somewhat akin to cultural products, such as the material legacies of the Italian Renaissance or Regency England: affectations of national pride that signal a distinct identity, create employment for members of an affiliate elite, and have little or no material geopolitical effect. Like the Pope and Buckingham Palace, the GDPR has no regiments. So its tightly leashed significance should not be overstated.

This sketch can be unpacked at least a little here. To begin with, digital regulatory policy in the United States, China, and the EU is a matter of political economy, not primarily of ideas. It reflects the interests of an elite intent on marshalling and leveraging available institutional and material resources. These elites' influence cuts across the state and the corporate sector. Especially in a policy domain where technical advances occur in the private sector, and where governments (even China's) are de facto dependent on private firms as national champions, it makes little sense to think of the state acting *suo proprio moto*. Further, as a consequence of the same centrality of technical knowledge, the relevant elite here are not identical to the hegemonic group in foreign policy matters more generally.

To capture this distinctive idea, I would borrow Professor Gabrielle Hecht's concept of a "technopolitical regime."[293] On Hecht's definition of that term, it is a "linked set[ ] of people, engineering and industrial practices, technological artifacts, political programs, and institutional ideologies which act together to govern technological development and pursue technopolitics."[294] I find Hecht's concept useful here because it is not bounded by a

---

[293] Gabrielle Hecht, *Technology, Politics, and National Identity in France*, *in* TECHNOLOGIES OF POWER: ESSAYS IN HONOR OF THOMAS PARKE HUGHES AND AGATHA CHIPLEY HUGHES 253, 257–59 (Michael Thad Allen & Gabrielle Hecht eds., 2001).

[294] *Id.* at 257.

concern with specific officials or interest groups. The definition straddles the public-private line. It recognizes that their interests and strategies are shaped and directed by path-dependent histories of institutional design and technological choice. Put very crudely, the fact that Silicon Valley is in California, not the Ruhr or Shenzhen (or, for that matter, Alabama), matters: it determines the resources (including the possibilities for weaponizing interdependence) that a national technopolitical elite brings to bear in a given national context. These political economy dynamics matter far more than theories of regulation.

Having suggested ways in which the technopolitical regimes of the United States, China, and the EU might be characterized, I turn briefly to the way in which their choices are likely to be constrained by other spheres of geopolitical conflict. My aim in so doing is not to offer specific predictions, but simply to spell out a more perspicacious and useful analytic frame for thinking about the geopolitical dimension of digital regulation.

A. A Typology of Technopolitics

An understanding of global digital regulation thus starts with an approximation of the relevant technopolitical regimes. These are characterized by different mixes of public and private actors across the three jurisdictions. They can be labeled *digital political capitalism*, the *simulacra regulatory state*, and *party-state capitalism*.

The technopolitical regime of the United States is a form of digital political capitalism. U.S. officials and the leaders of tech firms act in tandem on the basis of many aligned or intertwined material and political interests. The U.S. state has a deep historical entanglement with the private digital economy that informs these opportunities and vulnerabilities.[295] The resulting dependency is bilateral in ways that shape these strengths and weaknesses.

On the one hand, private digital firms receive a wide array of subsidies and opportunities from the state explicitly intended to promote commercial innovation.[296] On the other hand, the U.S. state benefits through the creation, via private commercial activity, of what Farrell and Newman call weaponized interdependencies, which engender new ways to shape the geopolitical

---

[295] *See supra* text accompanying notes 183–200 (charting those linkages).

[296] *See supra* text accompanying notes 274–75.

environment.[297] The state thus comes to depend on those same firms for its domestic and foreign surveillance capabilities.[298] Moreover, because lists of "most valuable" U.S. firms are now dominated by Alphabet, Amazon, and Meta, the "future prosperity and geopolitical strength" of the nation is in some measure yoked to their fate.[299]

Yet at the same time, these very interdependencies conduce to unexpected vulnerabilities. Government relies on private companies to supply affordances such as email, for example, and then pays the toll when these firms experience security breaches.[300] And, as Kokas demonstrates, commercial reliance on the harvesting of personal data not only generates large profits for firms such as Meta and Google, it also creates striking geopolitical vulnerability via data exfiltration.[301] Because these firms and their business models are part of the dominant technopolitical regime in the United States, the data exfiltration problem is difficult, perhaps impossible, to solve through legislation. Such new law would necessarily constrain the reach of digital capitalists, drawing down their profits even as they mitigated a geopolitical weakness. It is hence to be expected that such measures (a category that includes the TikTok ban) would be limited or even nugatory in effect. This is an important internal contradiction of digital capitalism.

The label "digital political capitalism" draws upon Professors Dylan Riley and Robert Brenner's work on "political capitalism."[302] In brief, Riley and Brenner argued that since the 1970s, U.S. firms have responded to extended bouts of low productivity growth by seeking returns "not on the basis of investment in plant, equipment, labour[,] and inputs . . . , but rather on the basis of investments *in politics*."[303] In effect, they have looked to government as a wellspring of guaranteed income streams. The

---

297 *See supra* text accompanying notes 205–07.

298 *See, e.g.*, Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112 (2018) ("In today's world, government surveillance—whether targeted or programmatic, for law enforcement or foreign intelligence—relies on the cooperation of a small number of technology companies that are large, multinational, and opposed to it.").

299 Matthew J. Slaughter & David H. McCormick, *Data Is Power: Washington Needs to Craft New Rules for the Digital Age*, 100 FOREIGN AFFS., May/June 2021, at 54, 57.

300 Kevin Collier, *China-Based Hackers Breach Email Accounts at State Department*, NBC NEWS (July 12, 2023), https://www.nbcnews.com/tech/security/china-based-hackers-breached-email-accounts-microsoft-says-rcna93824.

301 KOKAS, *supra* note 8, at 8–17.

302 Dylan Riley & Robert Brenner, *Seven Theses on American Politics*, 138 NEW LEFT REV. 5, 6 (2022) (emphasis omitted).

303 *Id.* at 7 (emphasis in original).

result, explained Riley and Brenner, has been "massive state spending aimed directly at private industry," such as the CHIPS Act.[304] These investments "can be seen as an effort to generate an even larger profit stream."[305] Digital political capitalism is simply this concept transposed into a specific domain.

In contrast, the label "regulatory simulacra state" is meant to capture the idea of a jurisdiction that lacks the capacity to enforce laws *ex proprio moto* and does not have autochthonic firms to regulate directly. As a result of these gaps, regulation encounters neither of the ordinary frictions that renders it ineffectual. Neither the problem of enforcement nor the problem of political resistance ever need arise.

The EU fits this description because it is characterized by a weak governmental apparatus sitting alongside a weak digital private sector. On the one hand, as Bradford observes, the EU's reliance on regulation is "a result of the EU's small budget" and its relatively small institutional footprint.[306] In consequence, the EU itself does not have significant enforcement capacity. It instead depends on national authorities to make sure its rules are followed. This means, as the experience of GDPR enforcement gaps shows, that the efficacy of its legislative interventions cannot be taken for granted.[307] On the other hand, the EU also has a much less developed digital commercial sector than the United States or China.[308] (Hence the exorbitant hopes placed upon a single French AI company, Mistral.[309]) In consequence, digital regulation is not likely to engender political headwinds because of domestic opposition.

The enforcement gap and the absence of domestic opposition together engender a moral hazard problem. In effect, the EU can regulate harshly knowing that it does not need to pay the political costs that would ordinarily be triggered by minatory regulation, or the transaction costs of enforcement. Digital regulation, in other words, can be cheaply produced because many of the ordinary costs of legal rules are in effect externalized onto other private and public actors outside the jurisdiction. The blend of the

---

304 *Id.* at 6.

305 Matthew R. Keller & Fred Block, *The New Levers of State Power*, 7 CATALYST 9, 11 (2023).

306 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 131.

307 *Id.* at 139 (noting the "lackluster enforcement of the GDPR"); *accord supra* text accompanying notes 226–27.

308 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 108 (noting the absence of "large" European tech firms).

309 *See supra* text accompanying note 272.

weak state and the weak private sector, in other words, paradoxically conduces to more rather than less aggressive regulation. This can then be held up with an air of oblivious self-satisfaction as evidence of "the strength of liberal democracy as a model of government."[310] And for that reason, the label "regulatory simulacra state" is especially apt.

Finally, as Bradford notes, Chinese policymaking is dominated by a party-state that "commands, controls[,] and integrates all other political organizations and institutions in China."[311] The party-state is motivated primarily by concern about its survival, which dominates any concern about Chinese firms as such.[312] As a result, the party-state's economic governance became "'securitized,' such that political control over firms and risk management are prioritized over rapid growth," and the boundary between the state and private sector is increasingly "blurred."[313] As a result, it is common practice for the party-state to "mobilize commercial actors to advance Beijing's foreign policy goals."[314] There is no bilateral dependency, as in the U.S. case. As Bradford's account of the government crackdown on tech firms demonstrates, influence really flows just one way.[315] Rather than labeling this "state-driven," the pervasive institutional prioritization of party over private interests points toward the utility of "party-state capitalism" as a descriptively apt label.[316]

---

310 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 392. If nothing else, this turn of phrase evinced a peculiar blindness to the complex and large role that markets have placed in present and past liberal thought.

311 Ming Xia, *The Communist Party of China and the "Party-State"*, N.Y. TIMES, https://archive.nytimes.com/www.nytimes.com/ref/college/coll-china-politics-002.html.

312 Margaret M. Pearson, Meg Rithmire & Kellee S. Tsai, *China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity*, 47 INT'L SEC. 135, 142–43 (2022).

313 *Id.* at 136–37. Bradford describes this as the pursuit of "state sovereignty." BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 70. That seems correct, but imprecise.

314 JAMES REILLY, ORCHESTRATION: CHINA'S ECONOMIC STATECRAFT ACROSS ASIA AND EUROPE 19 (2021).

315 BRADFORD, DIGITAL EMPIRES, *supra* note 17, at 71. There are a range of mechanisms through which control is achieved. *See, e.g.*, Lauren Yu-Hsin Lin & Curtis J. Milhaupt, *China's Corporate Social Credit System: The Dawn of Surveillance State Capitalism?*, 256 CHINA Q. 835, 835–38 (2023) (documenting the emergence of a "social credit" system for corporations, focused on fidelity to the party-state, that works "to incentivize corporate fealty to the CCP's industrial and social policies"); William J. Norris, *China's Post–Cold War Economic Statecraft: A Periodization*, 50 J. CURR. CHINESE AFFS. 294, 296 (2021) (identifying formal state planning and "the closely controlled provision of capital" as mechanisms of state control).

316 Pearson et al., *supra* note 312, at 136.

B. Conflicting Technopolitics in Context

One of the lessons of *Trafficking Data* and *Underground Empire* is that efforts at digital regulation cannot be understood in isolation from their wider geopolitical and historical context. By historicizing the present moment, for example, Farrell and Newman show that present disputes over digital regulation are best understood in the shadow of states' earlier investments in global infrastructure. While U.S. power over internet traffic and the Eurodollar market are not interchangeable, they are complementary parts of the same arsenal, used to achieve similar geopolitical ends—including the "containment" of China.[317] Further, the pattern of Chinese data trafficking mapped by Kokas can be understood as a tactical response by the party-state to China's points of geopolitical weakness. It is a savvy effort, from China's perspective, to leverage an internal contradiction of the way in which data flows in relatively unregulated markets given the resources available to a nation in a historical posture of disadvantage.

These insights of Farrell, Newman, and Kokas can be generalized. Digital technologies are interleaved into several other domains of geopolitical confrontation. These overlaps are inevitable. Most obviously, private and public digital capacities bear on the possibilities of surveillance, espionage, and counterespionage. The Chinese military's significant investments in AI and robotics showcase the relation of digital advances and a primary determinant of geopolitical power—the possibility of coercive action. And digital capabilities are linked to the availability of primary resources. Transistors used to comprise semiconductors, for example, require rare minerals such as cobalt and germanium mined largely in the Congo and China, respectively.[318]

Of particular importance, digital regulation is deeply entwined with energy security. Surprisingly, none of the three books considered here identify the nexus between energy policy and digital capabilities. The nexus arises because digital technologies are extremely energy intensive. New developments in AI in particular demand exponentially increasing amounts of energy.

---

317 *See supra* text accompanying notes 140–55. On the relation of weaponized interdependence to the perceived threat of China, see generally Johannes Petry, *China's Rise, Weaponised Interdependence and the Increasingly Contested Geographies of Global Finance*, 1 FIN. & SPACE 49 (2024).

318 *China Controls the Supply of Crucial War Minerals*, THE ECONOMIST (July 13, 2023), https://www.economist.com/finance-and-economics/2023/07/13/china-controls-the-supply-of-crucial-war-minerals.

By some estimates, data centers account for some 1–1.5% of the world's electricity usage.[319] An annual supply of new Nvidia AI chips exhausts "more than what many small countries use in a year."[320] Each new iteration of generative AI uses orders of magnitude more energy than the last. GPT-4, for example, took fifty times as much energy to train as GPT-3: some fifty gigawatt-hours, or 0.02% of the electricity the state of California generates in a year.[321] As a result, data centers and the networks used to transfer data are "a primary driver of global energy consumption."[322]

The resulting demands are reshaping national energy policies. In the United States, it is expected to drive a significant increase in the scale of natural gas production in coming years.[323] China is building a new electrical grid that allows it to shift from coal-fired to renewable sources. The continuous monitoring and control mechanisms this transition entails, however, are extremely vulnerable to cyberattack.[324] Energy security, which is necessary to digital capabilities, hence creates new kinds of digital vulnerabilities. Given these underlying trends, it seems increasingly implausible to talk about the geopolitics of digital technology, as these three books have done, without understanding their integration into the older, and more bloody, geopolitics of energy access and usage.

Conflicts over access to energy, oceanic trade routes, and military power are likely to dominate the strategic calculations of China and the United States into the near future.[325] In contrast, lacking both energy stocks and military capacity, Europe is already

---

319 Lauren Leffer, *The AI Boom Could Use a Shocking Amount of Electricity*, SCI. AM. (Oct. 13, 2023), https://perma.cc/GBB9-D977.

320 *Id.*

321 Ariel Cohen, *AI Is Pushing the World Toward an Energy Crisis*, FORBES (May 24, 2024), https://www.forbes.com/sites/arielcohen/2024/05/23/ai-is-pushing-the-world-towards-an-energy-crisis/; *see also* Andrew R. Chow, *How AI Is Fueling a Boom in Data Centers and Energy Demand*, TIME (June 12, 2024), https://perma.cc/GQF4-BKCJ (anticipating a doubling in energy demands from global data centers from 2022 to 2026).

322 Cohen, *supra* note 321.

323 Spencer Kimball, *AI Could Drive a Natural Gas Boom as Power Companies Face Surging Electricity Demand*, CNBC (May 5, 2024), https://perma.cc/H4ZA-R2VR.

324 TOM STEFANICK, BROOKINGS INST., SECURE POWER: GIGAWATTS, GEOPOLITICS, AND CHINA'S ENERGY INTERNET 1 (2020) (available at https://perma.cc/6KRZ-X3FW).

325 For an excellent synoptic explanation of these dynamics, see Helen Thompson, *The New Great Game*, THE NEW STATESMAN (May 22, 2024), https://www.newstatesman.com/international-content/2024/05/the-new-great-game-america-china-helen-thompson.

sidelined by these conflicts.[326] It must react, rather than act. Initiatives on energy and military power are likely to take primacy over digital policy under any foreseeable geopolitical conditions. A great power can operate, perhaps, without generative AI. Oil and guns are another matter entirely. This prioritization means that digital policy will unfold under constraints imposed by the other margins of geopolitical conflict and will continue to unfold in ways that are subservient to other security imperatives respecting energy, raw materials, and money.

Perhaps surprisingly, all this does not necessarily mean less digital regulation. To the contrary, the relatively lower geopolitical stakes of digital regulation may well make it easier for nations and groups of nations to reach agreement on certain policy questions.

A regulatory simulacra state such as the EU will continue to find it relatively cheap to produce rights-driven regulation as a sort of cultural export. Absent any real margin of maneuver between hegemonic powers, Europeans can regulate as a kind of compensatory or propitiatory virtue signaling. Regulation is a way of insisting, anachronistically, on the continued virtue and relevance of Europe in an era in which older liberal aspirations for the global order are rapidly collapsing.[327] Party-state capitalism, in contrast, is likely to see digital regulation as a way of responding to domestic discontents fed by rapid and disorienting economic change—until, that is, such demands are perceived as threatening the Communist Party's domestic political hegemony. Selecting off-the-shelf solutions that other jurisdictions have hammered out, as the party-state has done in the privacy context, is simply a low-cost and low-risk way of achieving that end.[328] In any case, there is no particular reason to think that digital regulations designed to respond to popular anxieties about technology will differ greatly from jurisdiction to jurisdiction. After all, it seems unlikely that the popular anxieties driving such measures vary in quality from one place to another. And if that is the case,

---

[326] On Europe's dependency for fossil fuels on Russia, see Christophe-Alexandre Paillard, *Russia and Europe's Mutual Energy Dependence*, 63 J. INT'L AFFS. 65, 65–66 (2010), and on military weakness, see Hugo Meijer & Stephen G. Brooks, *Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back*, 45 INT'L SEC. 7, 42 (2021) (concluding that "strategic cacophony and capacity gaps, which are mutually reinforcing," mean that "Europeans are currently not in a position to autonomously mount a credible deterrent and defense against Russia").

[327] G. John Ikenberry, *The Next Liberal Order*, 99 FOREIGN AFFS., July/Aug. 2020, at 133, 139.

[328] *See supra* text accompanying notes 253–55.

the emergence of a parallel regulatory solution should not be particularly surprising.

Finally, the United States will pursue its strategic goals through domestic regulation—but only to the extent that government is able to overcome its powerful local tech sector. Congress's recent singling out of TikTok,[329] ignoring much of the data exfiltration from other platforms and apps, suggests how these imperatives may be shaped in illogical and perverse ways by the strength of the commercial sector in digital political capitalism.[330] If TikTok survives (a question in some doubt as I write), it will be a consequence of the internal contradictions of digital political capitalism. These internal tensions will make it impossible to address comprehensively the extensive data exfiltration that Kokas describes so well. They turn national security into a hollow, and at times farcical, species of Kabuki. Otherwise, how to explain the persisting use of social media tools that present the same, or even greater, threats of data exfiltration as TikTok? And how to explain the way U.S. firms continue to seek "loopholes, third parties, and dummy companies" to enable technology transfers to China?[331]

All these jurisdictions, in short, have continued, powerful motives to enact domestic digital regulation. The latter will often be similar in effect but diverge in form. Moreover, as bilateral conflict between the United States and China potentially increases (as seems likely, especially given the mercurial and myopic foreign policy of the new Trump administration), there is every reason to think they will invest increasingly in efforts to shape the next generation of digital infrastructure—whether it be through the Belt and Road Initiative, domestic subsidies for semiconductor fabrication plants, or knife fights over the technical standards for 5G and the internet of things.

Ours, in short, may indeed be a golden age for digital regulation. Whether that is cause for celebration, though, remains in legitimate doubt. The laws that will be produced, marked out by

---

[329] *See supra* text accompanying notes 1–2.

[330] In § g(3)(A)(ii), PAFACA explicitly names TikTok, but in § g(3)(B)(ii) also permits the President to designate any "foreign adversary controlled application" if it presents a "significant threat to the national security of the United States." PAFACA, 138 Stat. at 958–59. As Kokas's analysis suggests, the most obvious candidates for such designation are WeChat and gaming companies such as Epic Games (owner of Fortnite) and Riot Games (owner of League of Legends). However, the only nationality of firms plausibly amenable to designation under this provision is China. KOKAS, *supra* note 8, at 115–16, 122–26, 130–32.

[331] Richard Beck, *Bidenism Abroad*, 146 NEW LEFT REV. 5, 18 (2024).

the quiddities of different technopolitical regimes, are hardly likely to be designed uniformly with the advancement of human welfare in view. They will, in any case, be forged in the margins of geopolitical conflict that is increasingly likely to take a toll not in missing imports but lost lives.

CONCLUSION

The geopolitics of digital regulation will continue to shape the ways in which the United States, European Union, and China alike discipline domestic regulation of the burgeoning social, commercial, and governmental uses of digital tools. *Digital Empires*, *Trafficking Data*, and *Underground Empire* each provides a unique and valuable vantage point on the prospects for such regulation. *Digital Empires* in particular provides a powerful synoptic typology for understanding that global context. Put side by side, these contributions cast even more light on, and point toward potentially more perspicacious ways of, recasting out typologies of digital regimes so as to better understand the perilous and murky terrain the world now seems intent on exploring. While all three books antedate the second Trump presidency (like this Book Review), the changes to the geopolitical landscape wrought by the new administration can profitably be evaluated through the analytic tools developed in these volumes. At least on initial inspection, the new landscape may be especially amenable to appraisal in terms of a clash of technopolitics. In particular, the U.S. strain of digital political capitalism apparent in the first months of 2025 seems an especially vivid, even hypertrophic, manifestation of the political form described here. Its evolution, though, remains to be charted.

My aim in this Book Review has been to praise the insights offered by these volumes and advance our understanding of these dynamics with a refined version of Bradford's model. No doubt this is not the last word. But my hope is that it gets us closer to an accurate understanding of the global dynamics of digital regulation before that world unravels entirely before our eyes.