CYBERBORDERS: EXERCISING STATE SOVEREIGNTY ONLINE

Beth A. Simmons[*] *& Rachel A. Hulvey*[*]

The internet brings challenges that threaten national identities and the foundations of what it means to be a state. Well-known challenges include difficulties maintaining important national values, competition threatening local economic plans, and even the inability to maintain a meaningful informational environment for self-governance. These influences are plausibly understood as challenges to some of the basic functions of a sovereign state. Despite these challenges, we identify the social practice of establishing control over mercurial mediums. States have responded by erecting cyberborders with a collection of laws, practices, and internet architecture designed to filter digital information within the territorial jurisdiction of the state. We contend that new digital bordering methods largely reflect and reproduce the territorial identity of the state. Border allusions, informed by concepts of geography, walls, and territoriality, are rife in states' official internet rhetoric. In policy and practice, states are not only guided by vertical relations between state and society, but also have horizontal orientations for controlling cross-border flows. We define these preferences as a state's border orientation or the underlying state preference for preserving national identity by filtering global forces. These preferences explain the rise of legal efforts to control the entry and exit of data and explain national approaches to sovereignty online across regime types.

> *"Within Chinese territory, the internet is under the jurisdiction of Chinese sovereignty. The internet sovereignty of China should be respected and protected."*
>
> White Paper, The Internet in China 2010[1]

[*] Andrea Mitchell University Professor in Law, Political Science and Business Ethics, University of Pennsylvania.

[*] Ph.D. Candidate, Department of Political Science, University of Pennsylvania. For helpful feedback, the authors would like to thank Duncan Hollis, Christopher Yoo, and participants in the Temple Law's Institute for Law, Innovation & Technology (iLit) and *Temple Law Review* Symposium. The authors also thank Beatrice Karp, Eleanor Stalick, and Michelle Wan for providing invaluable research assistance and the University of Pennsylvania Law School for providing generous funding to support this research. All errors are our own.

1. White Paper on the Internet in China, Information Off. of the State Council of the People's Republic of China (2010), https://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm [https://perma.cc/683W-FW5Q].

TABLE OF CONTENTS

INTRODUCTION 618
I. THE DIGITAL AGE AND THE SOVEREIGN IDENTITY CRISIS 620
A. The Crisis 620
B. The Response 622
II. ROOTS OF A RESPONSE TO THE SOVEREIGN IDENTITY CRISIS 624
A. Border Orientation 624
B. Building Borders, Virtual and Real 626
III. HOW STATES ENACT CYBERBORDERS 627
A. Data Localization 627
B. Takedown Requests 631
C. Foreign Website Blocking 634
D. Discussion: Cyberborders and Terrestrial Borders 638
CONCLUSION 639

INTRODUCTION

Territorial states are increasingly overtaken by a sovereign identity crisis. The integration of markets, the mobility of humans, and the instantaneous transfer of information across borders represent massive opportunities but also challenge states' abilities to govern territorially. On the one hand, globalization has enabled societies to enjoy a broad range of products and services, interact with different cultures, and share new ideas. On the other hand, the state's identity is rooted in the provision of collective goods for a people in a specific territorial location. When it appears unable to do so, the territorial state's *raison d'etre* comes into question.

Are states facing a "sovereign identity crisis" in the digital age? Potentially, yes. We conceive of a state's identity as comprised of three components: functional, ideational, and spatial. Functionally, states aggregate and coordinate human efforts to achieve collective goods, such as defense, education, public order, or economic development.[2] Ideationally, states cultivate cultural and other socially shared values of their dominant population.[3] They instantiate the social purposes of their citizens.[4] And finally, states' identities are spatial. They occupy physical territory on earth where their jurisdictional authority is broadly recognized.[5] No other authority in the modern world,

2. Charles Tilly, *Reflections on the History of European State-Making*, *in* THE FORMATION OF NATIONAL STATES IN WESTERN EUROPE 3, 3–89 (Charles Tilly ed., 1975).

3. BENEDICT ANDERSON, IMAGINED COMMUNITIES: REFLECTIONS ON THE ORIGIN AND SPREAD OF NATIONALISM (Verso Books 2006).

4. *Id.*

5. *See* Montevideo Convention on the Rights and Duties of States, art. 1, Dec. 26, 1933, 49 Stat. 3097, T.S. 881, https://www.hlrn.org/img/documents/Montevideo_Convention.pdf [https://perma.cc/HEX7-9WMP] ("The state as a person of international law should possess the following qualifications: a) a permanent population; b) a defined territory; c) government; and d) capacity to enter into relations with the other states.").

whether personal or spiritual, has territoriality as its defining feature.[6] States can be said to experience a sovereign identity crisis when their ability to promote collective effort, protect national cultural values, or govern spatially is seriously challenged.

Territorial sovereignty describes the right of the modern state to regulate activities, people, and ideas according to social purposes on its territory. When they cannot do so effectively, this produces anxiety about sovereign identity which is the focus of this forum. Uncontrollable interdependence across jurisdictions raises questions about why we should consider the territorial state as the locus of sovereign governance. In this sense, neoliberal globalization presents the state with a crisis of governability[7] and undermines the very legitimating mission of the state itself.

Historically, modern states have responded by erecting borders, i.e., "bordering." In practical terms, this has meant delimiting, enforcing, and hardening the boundary of their territorial jurisdiction. Political entities from city-states to empires have been defining and defending territorial borders for centuries to keep out unwanted people, products, and multifarious threats.[8] The use of territorial bordering technologies are widely viewed as a legitimate exercise of state authority. Wendy Brown has argued persuasively that border hardening can, in fact, be understood as a response to challenges to state sovereignty.[9]

Many early commentaries on the digital age thought that uniquely among the forces of globalization, the digital age would be different. Digital media would be nearly impossible for states to block from view or to contain within the state. In this Essay, we contend on the contrary that a "splinternet"[10] has been engineered by sovereign territorial states to maintain their territorial distinctiveness.[11] Well over a decade ago, Goldsmith and Wu noted that many states had the technological capacity to filter internet traffic according to territory.[12] Building on their prescient insights, we make the more provocative argument that physical and cyberborders are of a piece. Both address anxieties that the sovereign state will be overwhelmed by global forces. Moreover,

6. Beth A. Simmons & Hein E. Goemans, *Built on Borders: Tensions with the Institution Liberalism (Thought It) Left Behind*, 75 INT'L ORG. 387, 387–410 (2021); Jordan Branch, *Mapping the Sovereign State: Technology, Authority, and Systemic Change*, 65 INT'L ORG. 1, 1–36 (2011).

7. Nira Yuval-Davis, *The Double Crisis of Governability and Governmentality: Potential Political Responses to Living in a Risky Global Environment*, 52 SOUNDINGS, Winter 2012, at 88.

8. CHARLES S. MAIER, ONCE WITHIN BORDERS: TERRITORIES OF POWER, WEALTH, AND BELONGING SINCE 1500, at 16, 65, 67 (2016).

9. *See generally* WENDY BROWN, WALLED STATES, WANING SOVEREIGNTY (Zone Books 2010).

10. *See* Michael Grothaus, *Get Ready for the "Splinternet": The Web Might Not be the Worldwide Much Longer*, FAST COMPANY (Sept. 7, 2018), https://www.fastcompany.com/90229453/get-ready-for-the-splinternet-the-web-might-not-be-worldwide-much-longer [https://perma.cc/YV22-PYZV].

11. *Id.*; Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOB. LEGAL STUD. 475 (1998); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998). For a general discussion of territorial sovereignty in cyberspace, see Wolff Heintschel von Heinegg, Legal Implications of Territorial Sovereignty in Cyberspace (4TH INT'L CONF. ON CYBER CONFLICT 2012), https://securitypolicylaw.syr.edu/wp-content/uploads/2015/06/Heinegg_Sovereignty_In_Cyberspace.pdf [https://perma.cc/T792-V7XA].

12. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 149–50 (2006).

cyberborders and terrestrial borders rest on similar classes of technologies, from law to bureaucracy to architecture, that the state has historically developed to preserve its sovereign identity. We deploy the concept of *border orientation*, which is a deep-seated, state-cum-society preference for jurisdictional distinctiveness.[13] This slow-moving preference is not directly observable but is evidenced by a broad range of state projects designed to control global influences. Empirical research has shown there is a statistically significant correlation between states' physical border barriers on land—such as walls, fences, border police, and inspection facilities—and the erection of cyberborders.[14] Both kinds of bordering projects spring from the same preference for protecting the local while filtering the global.[15] Border walls and cyberborders both respond to challenges to the sovereign identity crisis of the modern territorial state.

Section I explores the link between the digital age and crises of sovereign identity and documents the central role that spatial thinking plays in states' cyber strategy. Section II defines the concept of border orientation and draws out the commonalities between cyberborders and terrestrial border fortifications. Section III discusses how cyberborders are implemented in law and practice. We conclude that states vary significantly in their preferences for jurisdictional distinctiveness, and that cyberbordering represents an effort by territorial states to preserve their identity and authority through the age-old impulse to differentiate through bordering.

I. THE DIGITAL AGE AND THE SOVEREIGN IDENTITY CRISIS

A. The Crisis

There is nothing new about the challenges extra-territorial forces pose to the territorial state. Integrated markets have complicated states' ability to control macroeconomic conditions and the distribution of wealth. Highly mobile foreign populations have complicated states' control over the entry of unwanted persons. Digital flows of transborder information have all affected states' ability to preserve local values (religious beliefs, cultural cohesion, civility, gender roles, privacy) and to ensure local governance integrity threatened by foreign launched fraud or misinformation. In short, states have repeatedly found it difficult to do what their territorial identity demands: to govern effectively within their territorial borders.

The digital age provides a host of examples. Citizen data is often stored in foreign data centers controlled by global firms but inaccessible to national industries and law enforcement.[16] In such cases, national privacy protections are largely beyond state control.[17] Data control has obvious commercial implications as well. Control over

13. Beth A. Simmons & Michael R. Kenwick, *Border Orientation in a Globalizing World*, 66 AM. J. POL. SCI. 853 (2022).

14. Rachel Hulvey & Beth Simmons, Cyberborders: Managing Interdependence in the Information Age (2022) (unpublished manuscript) (on file with authors).

15. *Id.*

16. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 369 (2015).

17. JENNIFER DASKAL & JUSTIN SHERMAN, DATA CATALYST INST., DATA NATIONALISM ON THE RISE: THE GLOBAL PUSH FOR STATE CONTROL OF DATA (2020).

commercial data drastically affects economic competition between local firms and global technology companies, which likely explains why India's telecom secretary Aruna Sundararajan stressed the strategic importance of controlling data: "We don't want to build walls, but at the same time, we explicitly recognize and appreciate that data is a strategic asset."[18] Such recognition has driven some states to prevent data exportation, citing national strategic interests.

Defining and enforcing rights is a key state function, and the internet challenges a state's ability to protect these freedoms. Enforcing intellectual property rights is a key example.[19] The proliferation of file-sharing tools has spawned copyright violations, and, as early as the 1990s, industries began to demand penalties and sophisticated digital enforcement measures to protect their intellectual property online.[20] More generally, an essential purpose of the state is to defend the prevalent social values of its population. Saudi Arabia, for example, systematically blocks internet content, including "provocative attire," Bahai faith, and content perceived as "insulting to the Islamic religion."[21] Many states attempt to control content that contravenes local social values of decency, such as hate speech, pornography, and defamation.[22] Liberal states in Europe control the export of information that risks their citizens' privacy.[23] Unfiltered global information introduces new ideas, some of which are likely to be seen as disgusting, dangerous, or socially dysfunctional in a particular cultural context.

Finally, global information poses new challenges to national security. For some states, the threats of disinformation and misinformation challenge the sanctity of elections and trust in the democratic process. Liberal states have encountered information that endangered the operation of democracy itself: eerily authentic-seeming forms of misinformation that incite political violence or diminish the legitimacy of elections.[24] "Deep fakes"—information and images that look authentic but falsely, egregiously, and

18. Vindu Goel, *India Pushes Back Against Tech* '*Colonization*' *by Internet Giants*, N.Y. TIMES (Aug. 31, 2018), https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html [https://perma.cc/ZVJ9-Q55Y].

19. These works emphasize the challenges of protecting property rights online. Shun-Yung Kevin Wang & Jeremy J McDaniel, *Piracy and Intellectual Property Theft in the Internet Era*, *in* ADVANCED METHODOLOGIES AND TECHNOLOGIES IN SYSTEM SECURITY, INFORMATION PRIVACY, AND FORENSICS (2019); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1975 (2006). Such concerns are especially strong among more liberal states whose citizens traditionally have tended to produce intellectual property and therefore value its protection. Mark P. McKenna, *Intellectual Property, Privatization and Democracy: A Response to Professor Rose*, 50 ST. LOUIS U. L.J. 829 (2005); Shoirahon Odilova & Xiaomin Gu, *Cognitive Abilities, Democracy and Intellectual Property Rights Protection*, 10 INT'L BUS. RSCH., no. 5, 2017, at 127.

20. LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE (Yale Univ. Press 2014); *see also* GOLDSMITH & WU, *supra* note 12. The Recording Industry of America reported music sales in the United States dropped from $14.6 to $7.7 billion after the advent of Napster, driving lobbying pressure from the bottom up. DENARDIS, *supra*, at 177.

21. *Internet Filtering in Saudi Arabia in 2004*, OPENNET INITIATIVE, https://opennet.net/studies/saudi [https://perma.cc/UJX4-7RZ7] (last visited Apr. 1, 2023).

22. Stuart Hannabuss, Book Review, 23 STRATEGIC DIRECTION, Oct. 2007 (reviewing GOLDSMITH & WU, *supra* note 12), https://doi.org/10.1108/sd.2007.05623kae.001.

23. Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018).

24. SARAH KREPS, SOCIAL MEDIA AND INTERNATIONAL RELATIONS 52, 69 (2020).

often salaciously threaten individuals, national security, and democratic institutions[25]—are an obvious target of concern for any liberal society. States also face significant threats from ransomware and cybercrime. Experts estimate that ransomware attacks will globally occur every eleven seconds, resulting in total damage costs of US$20 billion in 2021.[26] Developing countries are among the most vulnerable and most devastated by such attacks. In a matter of seconds, Bangladesh suffered an attack that stole US$81 million from the central bank, an amount that can shatter a state's development goals.[27] Economic damages from cybercrime are predicted to reach more than US$10 trillion annually by 2025, representing what some observers have called "the greatest transfer of economic wealth in history."[28]

B. The Response

How have territorial states attempted to govern in the face of such global information forces? They turn to familiar tools for making sense of the world. In particular, they develop means of securing the state territorially. Geography is central to the identity and existence of territorial entities. Their legitimate claim to rule inheres in a physical location where nationality and belonging are carved out by territorial boundaries. The geographic nature of state legitimacy is as true in cyberspace as it is on the ground. While the domain of struggle has changed from the physical to the digital, the first-order characteristic of states remains essentially territorial. To border is to differentiate, whether on *terra firma* or in cyberspace.

Bordering the internet is the policy response of choice because states think spatially, even when it comes to controlling digital information over the internet. Evidence of territorial thinking pervades states' strategic rhetoric regarding digital information. They use territorial metaphors to help bridge practices and understandings from offline to online spaces and use these metaphors to guide their thinking when responding to an emerging foreign challenge.[29] The very term "cyberspace" creates the imagery of a territory to be conquered.[30] "Domain" analogies have had a profound effect, for example, on United States military policy and the setup of a U.S. Cyber Command.[31] The idea of China's "Great Firewall," first coined over a quarter century ago, has stuck precisely

25. Robert Chesney & Danielle Citron, *Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?*, LAWFARE (Feb. 21, 2018), https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy [https://perma.cc/XFK3-R7QF].

26. *Ransomware Attacks, a Growing Threat that Needs to be Countered*, U. N. OFF. ON DRUGS & CRIME REG'L OFF. FOR SE. ASIA AND THE PAC. (Oct. 18, 2021), https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html [https://perma.cc/99L6-345A].

27. Rick Gladstone, *Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million*, N.Y. TIMES (Mar. 15, 2016), https://www.nytimes.com/2016/03/16/world/asia/bangladesh-bank-chief-resigns-after-cyber-theft-of-81-million.html [https://perma.cc/S5JA-K4AZ].

28. Steve Morgan, *Cybercrime To Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ [https://perma.cc/98UN-6NDL].

29. Jordan Branch, *What's in a Name? Metaphors and Cybersecurity*, 75 INT'L ORG. 39 (2021).

30. *Id.* at 41–49.

31. *Id.* at 50–56.

because of the power of the metaphor to capture the idea of exerting sovereign control over the internet *territorially*.

Evidence of a worldview grounded in physical and territorial ideas pervades national security documents. Turkey's National Cybersecurity Strategy contains spatial distinctions between national and international cyberspace,[32] and, in their domestic press, Turkish officials emphasize the need to defend cyberborders in addition to land, sea, and air space.[33] The Philippines' National Cybersecurity Plan includes a Cyber Geography Program to map national cyberspace infrastructure in a manner reminiscent of early cartographic efforts.[34] China's concept of cyber sovereignty is highly territorial.[35] China promotes the right of national governments to control the flow of information within national boundaries and regulate data according to the demands of national security.[36] China's National Strategy for Cyberspace describes cyberspace as a "new territory for national sovereignty,"[37] while their United Nations submissions extol the value of recognizing "all States have extended sovereignty to cyberspace."[38]

Spatial metaphors are also used to *oppose* policies of government control. The United States, for instance, has referred to a digital "Berlin Wall" to discourage states from interfering with free transborder flows of information.[39] Many countries remain similarly cautious about the ability to describe cyberspace in sovereign territorial terms.

---

32. MINISTRY OF TRANSP., MAR. AFFS. & COMMC'NS, REPUBLIC OF TURK., NAT'L CYBERSECURITY STRATEGY AND 2013-2014 ACTION PLAN 21 (2013), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/%281%29%20TUR%20NCSS%202013-2014.pdf [https://perma.cc/5T55-496J].

33. *See* Seda Sevencan, *Turkish President Shares Message on Digital Awareness*, ANADOLU AGENCY (Nov. 6, 2020), https://www.aa.com.tr/en/science-technology/turkish-president-shares-message-on-digital-awareness/1872812 [https://perma.cc/R9PX-PCXY].

34. PHILIPPINE NATIONAL CYBERSECURITY PLAN 2005, INT'L TELECOMM. UNION REPOSITORY OF CYBERSECURITY STRATEGIES (2005), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Philippine_2005_National%20Cyber%20Security%20Plan%202005.pdf [https://perma.cc/3BX8-U7F8].

35. Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107, 116 (Dennis Broeders & Bibi van den Berg, eds., 2020), https://ssrn.com/abstract=3532421.

36. Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty* 1 (Hoover Inst., Aegis Paper Series No. 1703, 2017); Adam Segal, *When China Rules the Web: Technology in Service of the State*, 97 FOREIGN AFFS. Sept.-Oct. 2018, at 10, 10–12.

37. 国家网络空间安全战略 [China's 2016 National Cyberspace Security Strategy], https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ [https://perma.cc/FJ7H-5XVX]. Original: https://www.qianxin.com/sitaw/down/国家网络空间安全战略全文.pdf "网络空间是国家主权的新疆域".

38. China's Views on the Application of the Principle of Sovereignty in Cyberspace, U.N. Open Ended Working Group Submission (2021), https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf [https://perma.cc/4YD5-WK2P].

39. *See*, *e.g.*, Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom at the Newseum (Jan. 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm [https://perma.cc/K2MB-WTH6] ("The Berlin Wall symbolized a world divided and it defined an entire era. Today, remnants of that wall sit inside this museum where they belong, and the new iconic infrastructure of our age is the internet. Instead of division, it stands for connection. But even as networks spread to nations around the globe, virtual walls are cropping up in place of visible walls.").

When discussing threats at the United Nations Open Ended Working Group on Information and Communications Technologies in 2019, Argentina noted, "cyberspace represents an intangible and global space with an infinite flow of data over which no dominion or sovereignty is exercised."[40] Love it or hate it, spatial sovereignty is the language of state governance. Through this lens, it is not surprising that states have deployed law, bureaucracy, and engineering techniques to border the internet. What may be more surprising is that a quantitative analysis found that there is a strong correlation between bordering a national territory with fences, walls, police stations, and well-defended border crossing stations and bordering the internet with data takedown requests, website blocking, and data localization requirements.[41] Bordering repertoires shape the policy space from which states draft policies and act.

II. ROOTS OF A RESPONSE TO THE SOVEREIGN IDENTITY CRISIS

A. Border Orientation

Analysts have largely interpreted the splintering of the internet in terms of censorship and repression, attributing most of it to authoritarian regimes. Analytical attention has focused largely on China, where internet controls are a tool to repress destabilizing forms of collective action that threaten the government,[42] censor social media,[43] and reinforce official versions of common knowledge.[44] Internet controls have largely been interpreted as a strategy of domestic repression to maintain political power uninhibited by free expression norms.[45] Most scholars assume authoritarian states possess comparative advantages to democratic ones in controlling the internet.[46] They assume that the most important relationship addressed by internet regulation is a vertical one between state and society.[47]

We suggest that the horizontal relationship between states provides even more leverage on why and where states attempt to regulate the internet. We draw on the concept of border orientation,[48] which is a preference for how a society is to be governed in the face of international forces: "It arises from the interplay of societal preferences and

40. Argentina, United Nations Open-Ended Working Grp. on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., Meeting 4, *Existing and Potential Threats* (2021) (transcript on file with the author).

41. Hulvey & Simmons, *supra* note 14. The traditional measure of borders draws from data based on geolocation using satellite imagery. *See* Simmons and Kenwick supra note 13.

42. *See generally* Gary King, Jennifer Pan & Margaret E. Roberts, *How Censorship in China Allows Government Criticism but Silences Collective Expression*, 107 AM. POL. SCI. REV. 326 (2013).

43. *See* Jonathan Hassid, *Safety Valve or Pressure Cooker? Blogs in Chinese Political Life*, 62 J. COMMC'N 212 (2012).

44. *See* MICHAEL SUK-YOUNG CHWE, RATIONAL RITUAL: CULTURE, COORDINATION, AND COMMON KNOWLEDGE *passim* (Princeton Univ. Press reissue 2013).

45. *See, e.g.,* DeNardis, *supra* note 20, at 15 ("In a significant portion of the world, Internet governance control structures do not embody democratic values but involve systems of repression, media censorship, and totalitarian surveillance of citizens.").

46. *See* KREPS, *supra* note 24, at 38–44.

47. *Id.*

48. *See generally* Simmons & Kenwick, *supra* note 13.

domestic institutions that aggregate and propagate actionable values more generally."[49] As institutions of public order, borders operate as "a means of realizing underlying preferences defined by the demands of societal groups."[50] In authoritarian regimes, border orientation will largely reflect the preferences of a dictator or "selectorate,"[51] but in more democratic countries, it results from the aggregation of broader state and societal preferences over national distinctiveness. However, this governance theory is distinct from traditional concepts of regime type. While the latter describes state-society ("vertical") relations, border orientation captures how the state/society governs forces emanating from the rest of the world ("horizontal" relations). As such, it demonstrates a preference for defining and protecting the home environment from the global one.

Border orientation preferences drive spatial policies designed to create national distinctiveness. It has traditionally been used to understand border hardening on the ground. We contend it is useful to alter the aperture of this concept to identify and analyze policies designed to create separation between foreign and national in a borderless medium. Such a national environment may be repressive in some cases, but in many instances, it is merely preferential or even "liberal." We contend this effort reflects the management of global forces more generally. Virtually and in the physical world, states create boundaries that simultaneously generate national identities and shore up the states' authority to govern. Governments are motivated to border the physical and virtual spheres to define the polity, regulate commerce, engender respect for local values, and curate ideas that distinguish "us" from "them." In this sense, bordering the internet is, like all boundary making, an attempt to engineer differences.[52]

Despite the technological challenges of regulating the internet, governments are "fencing" the internet for very traditional reasons: they want to maintain sovereign control over the information environment in their national territory. We contend that these practices have clear analogies in the physical world. The technologies differ, the bargaining power of states has changed, and the costs and benefits are not identical, but familiar concepts like walls, fences, and even territorial sovereignty continue to be useful. States struggle with sometimes overwhelming "cyber issues," but they are grounded in—and indeed are constituted by—territorial sovereignty. To understand recent trends toward internet fragmentation, we suggest it is important to think like a state. When we do, it becomes clear that state leaders have fairly traditional ideas and values about maintaining sovereign territorial control.

---

49. *Id.* at. 855.

50. Andrew Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, 51 INT'L ORG. 513, 525 (1997).

51. "Selectorate" is a term referring to the group that selects a leader in a political system without meaningful elections, for example in an autocratic state. The "selectorate" in an autocracy is analogous to the "electorate" in a democracy. Selectorate theory was first developed in Bruce Bueno de Mesquita, James D. Morrow, Randolph M. Siverson & Alastair Smith, *An Institutional Explanation of the Democratic Peace*, 93 AM. POL. SCI. REV. 791 (1999).

52. *See* Michèle Lamont & Virág Molnár, *The Study of Boundaries in the Social Sciences*, 28 ANN. REV. SOCIO. 167, 186–88 (2002).

B. Building Borders, Virtual and Real

To an astonishing degree, states use similar legal strategies of boundary making in cyberspace as they do in constructing their territorial borders. In both cases, bordering requires legal authorization, funding to construct and maintain, and legal definitions, rules, procedures, and permits to function. In most states, land border structures are erected "in a highly legalized fashion according to legal chains of authorizations."[53] Cyber bordering also involves the passage of laws, implementation of policies, and deployment of infrastructural investments designed to drive a wedge between the national information environment and that of the rest of the world. These laws are enforceable because states have the exclusive right to regulate the conditions under which firms, including multinational ones, operate in their territorial jurisdiction.

While it may be technically more difficult to control electronic data than humans or goods,[54] the purposes and commonalities are striking. Figure 1 illustrates the similarities between traditional national borders, aimed at regulating the flow of persons and products between countries, and cyberborders, designed to regulate information flows. The thick vertical line represents a border. Borders filter both outflows (depicted on the left) and inflows (depicted on the right), although the latter seem to be more salient in contemporary policy. The broad purpose of policies on the left is to control strategic assets. Policies on the right are designed to curate jurisdictional distinctiveness.

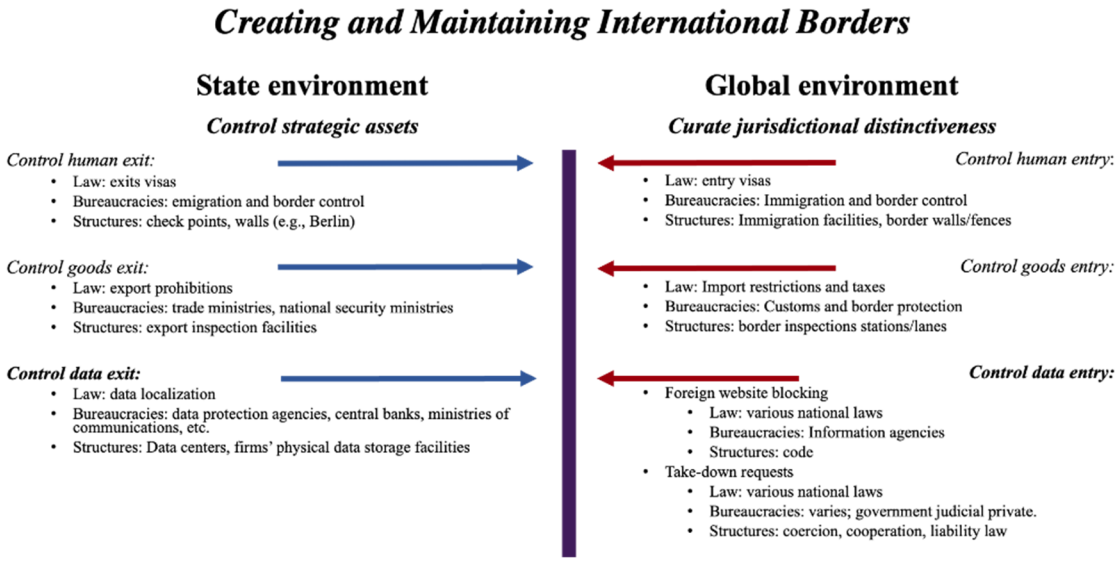

Figure 1. *Creating and maintaining international borders*. The goal of bordering is to create and maintain a national environment that is distinct from the rest of the world. Laws, bureaucracies, and structures filter and control the entry and exit of humans, goods, and information.

53. Yishai Blank, *Legalizing the Barrier: The Legality and Materiality of the Israel/Palestine Separation Barrier*, 46 TEX. INT'L L.J. 309, 317 (2011).

54. This is not obvious in all cases. Terrain, human motivations, and technical feasibility are all involved in the "success" of filtering cross-border movements.

III. HOW STATES ENACT CYBERBORDERS

At first glance, cyber bordering may appear to be a transnational bordering problem like no other. After all, digital information is nothing like a military tank, narcotics, or a human body. And yet policies to border the internet are strongly correlated with policies to border a state's territorial jurisdiction.[55] This is not because border walls, fences, and inspection stations "cause" cyberborders. It is because both territorial and cyber borders flow from a state's/society's preference, determination, and capacity for bordering generally. This claim has been recently supported with empirical evidence. Data gathered by Simmons and Kenwick[56] documenting gates, official buildings, inspection stations, border walls, border fences, and police stations in border zones provide evidence of hardening land borders around the world. Using this data reveals that "thicker" terrestrial borders positively correlate with at least three cyber bordering practices: *data localization laws, website blocking*, and *data takedown requests*.[57]

A. Data Localization

Governments design data localization laws to regulate what types of data can leave national jurisdiction. Data localization laws may prohibit, impound, or conditionally permit the export of certain types of data.[58] These laws are enforceable because states have the exclusive right to regulate the conditions under which firms, including multinational ones, operate in their jurisdiction, i.e., territorially. Even if the medium is complex, laws often place the burden on multinational firms to secure the infrastructure and data centers necessary to comply with national storage requirements.[59] Not all laws ban the same types of exports. Some impound particular types of data, some require security checks before outbound transfers, and some laws prohibit transfers to countries with insufficient privacy protections, for instance.[60]

Laws that restrict data export are clearly a bordering practice. The strictest laws demand exclusive national storage of data and require firms to make investments in data centers to impound data on national soil. For example, China's 2016 Cybersecurity Law[61] requires firms to store data collected on Chinese citizens exclusively within Chinese borders. In light of this requirement, Apple invested in a data center in Guizhou and also poured millions of dollars into a partnership with the local government to ensure the company would pass state security audits and manage data storage in compliance

55. Hulvey & Simmons, *supra* note 14, at 12–13.

56. Simmons & Kenwick, *supra* note 13.

57. Hulvey & Simmons, *supra* note 14, at 14.

58. *See generally* Alexander Zinser, *European Data Protection Directive: The Determination of the Adequacy Requirement in International Data Transfers*, 6 TUL. J. TECH. & INTELL. PROP. 171 (2004); Jinhe Liu, *China's Data Localization*, 13 CHINESE J. COMMC'N 84 (2020).

59. Daskal, *Borders and Bits*, *supra* note 23, at 234.

60. Anupam Chander, Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015).

61. 中华人民共和国网络安全法 [People's Republic of China Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016).

with national law.[62] National storage requirements also ensure that data is more accessible to the government when law enforcement needs to investigate crimes.

Requirements to impound national information within traditional boundaries are also motivated by industrial development policies. China, again, provides an example. President Xi Jinping has referred to data as a new factor of production.[63] Some laws are designed to encourage domestic industries to successfully use and benefit from national data. For example, the Reserve Bank of India (RBI) directed that financial and payment information be exclusively stored and processed within the national jurisdiction of India, to limit the advantages multinational firms' derive from analyzing digital transactions at centralized global locations.[64] American companies, including Visa and Mastercard, lobbied the RBI to alter the policy as the requirement undercuts their competitive advantages flowing from centralized processing in the United States.[65] The Indian digital payments firm, Paytm, saw such rules as necessary for leveling the playing field to foster "national wealth creation."[66] Since Indian firms strongly contested "data colonization" by American technology giants, they lauded regulations requiring Indian data to be managed by national firms rather than global corporations.[67]

Other countries eschew demands of full local data storage for more nuanced data localization requirements. In Europe, for example, the Data Retention Directive of 2006[68] was designed to regulate data retention where data had been generated or

62. Paul Mozur, Daisuke Wakabayashi & Nick Wingfield, *Apple Opening Data Center in China to Comply with Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html [https://perma.cc/G423-M9CP].

63. 习近平带政治局集体学习 领导干部要学懂用好大数据 [Xi Kinping Leading the Politburo to Learn Collectively. Cadres Should Learn to Understand and Use Big Data Well], CCTV, https://news.cctv.com/2017/12/10/ARTI3HNR1LMiMiNZKmr1NMD1171210.shtml [https://perma.cc/AF8Y-USLB].

64. The Srikrishna Committee Report notes benefits will be obtained from localization: "The growth of AI is heavily dependent on harnessing data" and "most of the personal data of Indian citizens, such as the data collected by internet giants such as Facebook and Google are largely stored abroad." COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS 92 (2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf [https://perma.cc/2SR8-XWEN].

65. *See* Vindu Goel, *U.S. Credit Card Giants Flout India's New Law on Personal Data,* N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/visa-mastercard-amex-india-data-law.html [https://perma.cc/3F8J-74HA].

66. Rana, *Paytm for Data Localisation Citing Privacy, Level Playing Field for Startups*, MEDIANAMA (Sept. 20, 2018), https://www.medianama.com/2018/09/223-paytm-data-localisation/ [https://perma.cc/BNA3-E59P]; *see also* Newley Purnell, *US Tech Giants Bet Big on India. Now It's Changing the Rules,* WALL ST. J. (Dec. 3, 2019) https://www.wsj.com/articles/u-s-tech-giants-bet-big-on-india-now-the-rules-are-changing-11575386675 [https://perma.cc/98V4-GE8W].

67. For reports of leveling the playing field, see Vindu Goel, *supra* note 65. For more on data colonization see Justin Sherman, *India's Data Protection Bill in Geopolitical Context*, NEW AMERICA (July 10, 2019), https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/indias-data-protection-bill-geopolitical-context/ [https://perma.cc/S43C-X5WR].

68. Directive 2006/24/Ec of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54.

processed in connection with the provision of publicly available electronic communications services or public communications networks. The Directive required EU states to store information on EU citizens' telecommunications data. However, the European Court of Justice (ECJ) struck down the directive in 2014 and found the objectives were not sufficiently tailored to preserve privacy in the face of increased government surveillance of information. Although the directive satisfied objectives of public interest and national security, the ECJ found it violated privacy protection contained in Article 8 of the European Convention on Human Rights.[69]

States vary significantly in their data localization laws and controlling the export of data is not the domain of one particular regime type. In the wake of the Cambridge Analytica scandal, where Facebook moved and processed citizen data abroad without consent, attention on the standards of outbound jurisdictions has increased.[70] One solution is to *impose spatial conditions on* which locations are permissible for data transfer. The most famous example is the European General Data Protection Regulation (GDPR),[71] which requires that firms obtain a data protection adequacy decision from the European Commission before transferring personal data to a third country.[72] The GDPR asserts the power of governments to prevent data from crossing borders if privacy protections are deemed inadequate. As European citizens associate being European with a strong level of privacy protection, the GDPR allows the EU to carve out a European vision of privacy and data protection in a borderless sphere.

69. *See* European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

70. Iga Kozlowska, *Facebook and Data Privacy in the Age of Cambridge Analytica*, HENRY M. JACKSON SCH. OF INT'L STUD., UNIV. OF WASH. (Apr. 30, 2018), https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/ [https://perma.cc/9WMR-E9XG].

71 . Council Regulation 2016/679, (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

72. *Id.* art. 45.

To illustrate the global variance, we have developed an original measurement of data localization laws using a database of legal texts maintained by InCountry,[73] a consulting firm that advises multinational corporations on storing and processing data in countries of operation. Data export restrictions include data localization laws that prevent firms from storing certain types of data abroad, such as health or financial data, as well as conditional transfer laws that restrict the movement of data to jurisdictions without stringent privacy protections. Figure 2 illustrates the global variation in the intensity of such laws.

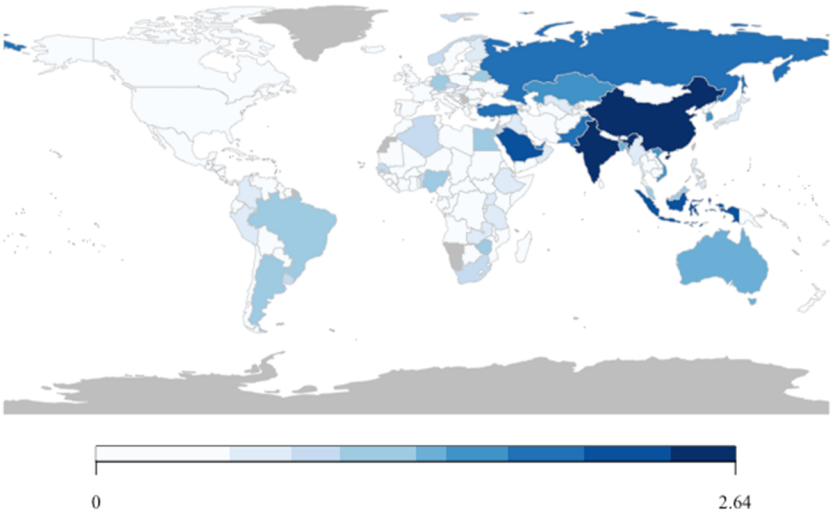

Figure 2. Data localization laws by country. Darker shades indicate more restrictive laws. Gray indicates missing data.

We find that the total intensity of data restriction laws worldwide positively correlates with Simmons and Kenwick's measure of terrestrial border structures.[74] The correlation suggests states and their societies desire to maintain jurisdictional distinctiveness by restricting outbound data flows. Sometimes this trend is motivated by a preference for maintaining privacy, typically reflected in conditional data transfer laws.[75] At other times, data localization laws reflect a desire to increase the state's capacity for surveillance to access data that would otherwise be stored on foreign servers.[76] In either case, the desire to filter and exclude traditional forms of cross-border

73. *Country Compliance Research Center*, INCOUNTRY, https://incountry.com/country-compliance/ [https://perma.cc/S43C-X5WR] (last visited Apr. 1, 2023).

74. Hulvey & Simmons, *supra* note 14, at 39 tbl.5.

75. Chris Jay Hoofnagle, Bart van der Sloot, & Frederick Zuiderveen Borgesius, *The European General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMMC'NS TECH. L. 65, 83–85 (2019), https://doi.org/10.1080/13600834.2019.1573501.

76. *See, e.g.,* COMM. OF EXPERTS UNDER THE CHAIRMANSHIP OF JUSTICE B.N. SRIKRISHNA, *supra* note 64, at 3–4.

movement is associated with a horizontal impulse to manage and separate the foreign from the domestic and to control national information.

B. Takedown Requests

States have a range of social and political motivations for attempting to reconfigure social media channels to maintain distinctions between domestic and foreign content. Many states work through multinational technology firms, such as Google or Facebook, altering the types of information displayed within national boundaries by issuing takedown requests.[77] Requests for removing certain kinds of foreign information from national view are usually based on national regulations for permissible forms of expression. For example, when Thailand demanded that YouTube filter videos of the king—which is illegal in Thailand but permissible in other jurisdictions—Google removed videos from their platform *only* within the geographic boundaries of Thailand, creating differences in the content to which users are exposed in different nations.[78] National security concerns motivate other requests to alter or elide digital information. South Korea has demanded that Google blur or hide sensitive locations such as power plants and military installations.[79] Some governments have even sought to reinforce their territorial claims on digital maps.[80] Google received a request from Vietnam to "correct" the boundaries of a Vietnamese providence near China and the firm adapted the details on Google Maps visible in Vietnam.[81]

Many states enforce the boundaries of permissible content through intermediary liability laws. Such laws require firms to respect distinctions in national culture and values and adapt platforms accordingly. Some legal models offer firms a safe harbor from liability in exchange for hiding infringing content once firms receive notice of content violating domestic rules, such as copyright protections.[82] In the United States,

77. Note takedown requests are different from the requests users submit or the self-regulatory policies of platform companies, including terms of service elegantly addressed by Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018).

78. *See id.* at 1623.

79. Jo He-rim, *Google Maps Exposes 40 Percent of South Korea's Military Installations: Lawmaker*, KOR. HERALD (Oct. 20, 2019), https://www.koreaherald.com/view.php?ud=20191020000188 [https://perma.cc/4A9K-7FY2].

80. Greg Bensinger, *Google Redraws the Borders on Maps Depending on Who's Looking*, WASH. POST (Feb. 14, 2020), https://www.washingtonpost.com/technology/2020/02/14/google-maps-political-borders/ [https://perma.cc/75ZG-Z4UL]. Computer scientists have systematized programs that detect and monitor "personalization" of online maps deemed suitable by states for their domestic audiences. *See* Gary Soeller, Karrie Karahalios, Christo Wilson & Christian Sandvig, *Mapwatch: Detecting and Monitoring International Border Personalization on Online Maps* (Int'l World Wide Web Conferences Steering Comm., Apr., 2016), https://cseweb.ucsd.edu/~gsoeller/publications/mapwatch-www2016.pdf [https://perma.cc/BQD5-5GQZ] (last visited Apr. 1, 2023).

81. *Government Requests to Remove Content*, *Vietnam Case*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/government-removals/government-requests?lu=request_country&request_country=authority:VN;p:2 [https://perma.cc/5NZV-B3MB] (navigate to the "Explore Requests" section at the bottom of the page, and for "Country/Region," select Vietnam).

82. Annemarie Bridy, *Copyright's Digital Deputies: DMCA-plus Enforcement by Internet Intermediaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 185, 186 (John A. Rothchild ed., 2016), https://doi.org/10.4337/9781783479924.00021.

the Digital Millennium Copyright Act[83] largely outsources handling disputes about intellectual property violations to platform companies that must then remove infringing content from their platforms once notified. These laws reinforce the ability of the state to protect intellectual property by requiring social media platforms to adapt global platforms when notified of violations. Intermediary liability laws also connect to many states' goals of maintaining a domestic environment free from incivility or violence.

Other intermediary liability models incentivize proactive policing by threatening to fine firms for illegal content transmitted or posted on the social network. Germany's NetzDG law[84] responded to heightened levels of online hate speech to mitigate the risk that online rhetoric will mobilize offline hate crimes. The law allows individuals to submit concerns directly to firms to remove any violative speech within Germany's borders.[85] Google's Transparency Reports reveal that individuals and businesses have requested a large number of takedowns for hate speech and violence viewable within their jurisdiction, suggesting strong societal interest in online civility.[86] Australia created laws to prevent the rapid dissemination of terrorist content on social media, in response to the Christchurch, New Zealand massacre the gunman had live streamed.[87] Australia's law requires multinational technology firms to police internet traffic for violent content and remove abhorrent material.[88]

Some laws direct content erasure rather than removal and reflect a concerted state response to protect cultural values. The European Union codified the "right to erasure" in the 2018 GDPR.[89] The "right to be forgotten" derives from a long history of the "right to oblivion" that arose as a means of protecting the dignity and privacy of individuals.[90] Under Article 7 of the Charter of Fundamental Rights of the European Union, individuals are protected from inappropriate communications that threaten to degrade, humiliate, or mortify them.[91] As search engines increasingly become the means of finding people online, what information appears on the first page of a search query can significantly impact someone's personal and professional life. Information found in the results shapes a stranger's estimations of that individual—creating the potential for humiliation or, in the extreme, the forfeiture of jobs or personal relationships. Intervention by the state

83. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860.

84. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerkdurchsetzungsgesetz] [NetzDG] [Network Enforcement Act], June 30, 2017, BUNDESGESETZBLATT TEIL I [BGBL I] (Ger.) [https://perma.cc/L3FEYZF3].

85. *Id.* at § 3(1).

86. *See Removals Under the Network Enforcement Law*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/netzdg/overview [https://perma.cc/Z2ZX-XQRG] (last visited Apr. 1, 2023).

87. Evelyn Douek, *Australia's 'Abhorrent Violent Material' Law: Shouting 'Nerd Harder' and Drowning Out Speech*, 94 AUSTL. L.J. 41 (2020).

88. *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) (Austl.).

89. Regulation 2016/679, *supra* note 71, art. 17.

90. *See generally* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (4th prtg. 2011).

91. Robert C. Post, *Data Privacy and Dignitary Privacy:* Google Spain*, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 982 (2018). This longstanding concept at stake is referred to as "dignitary privacy." *Id.*

draws a boundary around search engine results, so privacy-infringing content is not available within the European Union.

Figure 3 displays how intensively states around the world have used content removal and takedown requests to filter global information that would otherwise be visible domestically. For each country in the world, we used Google's Transparency Reports[92] to document the frequency of content removal requests made to Google between 2011 and 2021. Each request represents a demand to distinguish the content that social media and search engines offer nationally versus globally by removing content visible within the state's jurisdiction. States work through multinational firms to border the world wide web in an effort to maintain a distinct domestic informational environment. Recent research has found that the intensity of takedown requests states make is correlated with the intensity of states' physical border architecture in place around the world.[93]

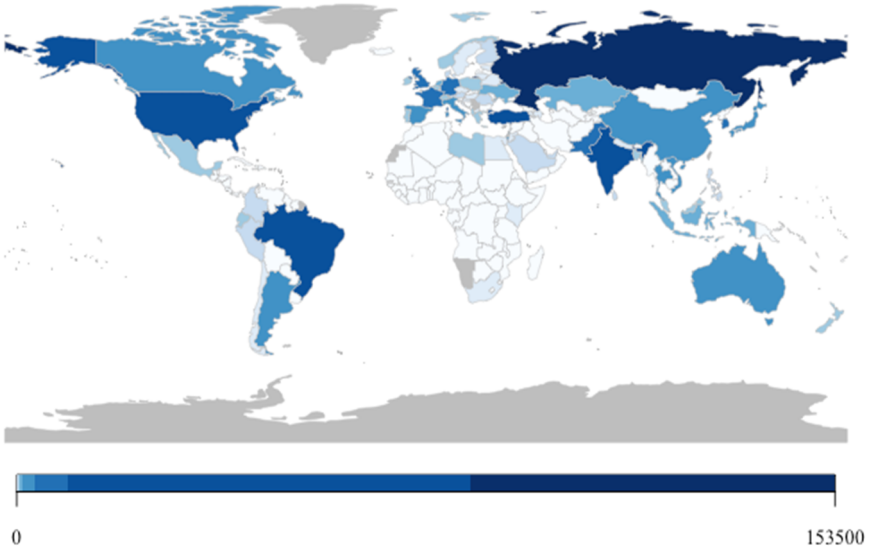

Figure 3. *Google content removal requests*. The number of requests states have made to Google to remove content from their platform, total, 2011–2021. Gray indicates missing data**.** Russia is by far the most frequent content removal requestor. Even democracies such as the United States, Australia, and France have made a significant number of takedown requests. China, which blocks Google wholesale, has also made ad hoc requests.

92. GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/ [https://perma.cc/77AB-PMFY] (last visited Apr. 1, 2023).

93. Hulvey & Simmons, *supra* note 14, at 29, tbl.2.

C. Foreign Website Blocking

Takedown requests described above are a "retail" approach to cyber bordering; states issue individual requests to private firms to remove illegal or unwanted content on a case-by-case basis. Website blocking is a "wholesale" approach. States wall off their territory from global information by blocking foreign websites rather than requesting the removal of specific content. Blocking foreign websites reflects an even more intense desire of the state to control how and where citizens are exposed to foreign ideas, products, and transactions. Many authoritarian states blocked foreign social media platforms, such as Twitter and Facebook, in the wake of the Arab Spring protests that had been organized on such channels.[94] During its invasion of Ukraine, Russia blocked American and Ukrainian websites to sever the domestic information space from global news critical of Russia's attack.[95] Others report on the construction of digital walls during the pandemic and governments' desires to control how global news about the virus was consumed by domestic populations. China blocked global news on the COVID-19 pandemic from crossing China's borders.[96] Democracies block and shut down websites that violate intellectual property protections in a similar manner to the seizure of drugs or other illegal substances.[97]

Erecting digital walls by blocking the visibility of specific websites requires state investments in infrastructure.[98] State-created infrastructure includes engineering code that redirects internet traffic through deep packet inspection technology looking for illegal content and malicious intent.[99] Firewalls require sophisticated routers to redirect internet traffic data at a number of limited "gateway" protocol points, similar to gates at land ports of entry.[100] Would-be entrants are denied access, effectively walling off parts of the global internet for users within territorial boundaries.[101]

Website blocking is not a matter of engineering alone. Law is at the center of strategies to control how domestic internet users interact with foreign content. Russia's Sovereign Internet Law,[102] for example, targets internet exchange points (IXPs) where

94. *See generally* Sean Aday, HENRY FARRELL, MARC LYNCH, JOHN SIDES & DEEN FREELON, U.S. INST. OF PEACE, BLOGS AND BULLETS II: NEW MEDIA AND CONFLICT AFTER THE ARAB SPRING, PEACEWORKS NO. 80, (2012) (analyzing the effects of the Arab Spring protests on news media); Eva Bellin, *Reconsidering the Robustness of Authoritarianism in the Middle East: Lessons from the Arab Spring*, 44 COMPAR. POL. 127 (2012).

95. Adam Satariano & Valerie Hopkins, *Russia, Blocked From the Global Internet, Plunges Into Digital Isolation*, N.Y. TIMES (Mar. 7, 2022), https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html [https://perma.cc/L53W-SDS9].

96. Yingdan Lu, Jack Schaefer, Kunwoo Park, Jungseock Joo & Jennifer Pan, *How Information Flows from the World to China*, 2022 INT'L J. PRESS/POL. ONLINEFIRST 1, https://doi.org/10.1177/194016122211174.

97. *See* Laura DeNardis, *Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance*, 15 INFO., COMMC'N & SOC'Y 720 (2012).

98. *See id.*

99. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 55 (1999).

100. GOLDSMITH & WU, *supra* note 12, at 92–93.

101. For active monitoring of blocking strategies in China as they constantly evolve, see GREATFIRE, https://en.greatfire.org/ [https://perma.cc/2Y26-HK7J] (last visited Apr. 1, 2023).

102. FEDERAL'NΓZAKON VNECENII IZMENENII V FEDERAL'NYI ZAKON O SVYAZII I FEDERAL'NYΓZAKON OB INFORMATSII, INFORMATSIONNIX TECHNOLOGIYAX I 0 ZAZHITYE INFORMATSII [Federal Law No. 90-FZ of May 1, 2019 "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information,

hundreds of internet service providers (ISPs) connect. The law prohibits ISPs from using IXPs located in neighboring countries, so Russia can, in theory, shield domestic internet usage from outside threats, competition, and dependencies, but this requires significant investment to reroute global traffic.[103] China's Great Firewall is a collection of laws and practices that distinguishes China's national information from the rest of the world. Even the United States—one of the most liberal free speech countries in the world—has legislation that blocks websites that promote human or sexual trafficking.[104]

Governments often work with ISPs by providing a list of URLs or categories of websites that should be blocked within the state's jurisdiction. One example is India's 2009 Information Technology Procedure and Safeguards for Blocking for Access of Information by Public Rules.[105] These rules empower the central government to direct any agency or intermediary to block access to information when satisfied that it is "necessary or expedient" for the "sovereignty," "integrity," or "[d]efence," of India, "[s]ecurity of the State," "[f]riendly relations with Foreign States," "public order" or "[f]or preventing incitement to the commission of any cognisable offence relating to above."[106]

The incidence of website blocking varies significantly around the world. To demonstrate this, we collected data on blocking incidents from the world's top 500 websites (by traffic).[107] We then collected evidence gathered by the Censored Planet Project on traffic disruptions to these major sites.[108] Finally, we used SimilarWeb's categorization of each website's content to draw inferences about the motivations for blocking. The results are displayed in Figure 4. Some countries, such as China, Saudi Arabia, and Afghanistan, block foreign websites in almost every category displayed. But even liberal western democracies, such as Canada, Australia, and Norway, block certain

Information Technologies and Information Protection"] SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOI FEDERATSIĬ [SZ RF] [Russian Federation Collection of Legislation] 2019, No. 18, Item 2214, http://publication.pravo.gov.ru/Document/View/0001201905010025 [https://perma.cc/5QMQ-CHTP].

103. Charlotte Jee, *Russia Wants To Cut Itself Off from the Global Internet. Here's What that Really Means*, MIT TECH. REV. (Mar. 21, 2019) https://www.technologyreview.com/2019/03/21/65940/russia-wants-to-cut-itself-off-from-the-global-internet-heres-what-that-really-means/ [https://perma.cc/S6FT-52KK].

104. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (codified as amended in scattered sections of 18 and 47 U.S.C.) (2018). This legislation has led to the closure of Craigslist personal pages, among others. Aja Romano, *A New Law Intended To Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July, 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom [https://perma.cc/3MF9-QBUA].

105. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R 78 E. (India), https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%2C%202009.pdf [https://perma.cc/YZ3Y-9YK2].

106. *Id.*

107. Data are from SimilarWeb. *See Top Websites Ranking*, SIMILARWEB https://www.similarweb.com/top-websites/ [https://perma.cc/XYV3-ZS3E] (last updated July, 2022). For details, see Hulvey & Simmons, *supra* note 14, and associated appendices.

108. CENSORED PLANET, https://censoredplanet.org/ [https://perma.cc/9V4U-LGWA] ("An Internet-wide Longitudinal Censorship Observatory"); *see* Hulvey & Simmons, *supra* note 14, and associated appendices for details.

websites, especially those that facilitate file sharing—and thus potential property rights violations—and certain social media sites. Research demonstrates that blocking social media, file transfer, news media, commerce, and culture/streaming websites are all positively correlated with physical border architecture more generally.[109]

109. Hulvey & Simmons, *supra* note 14, at 35 tbl.4.

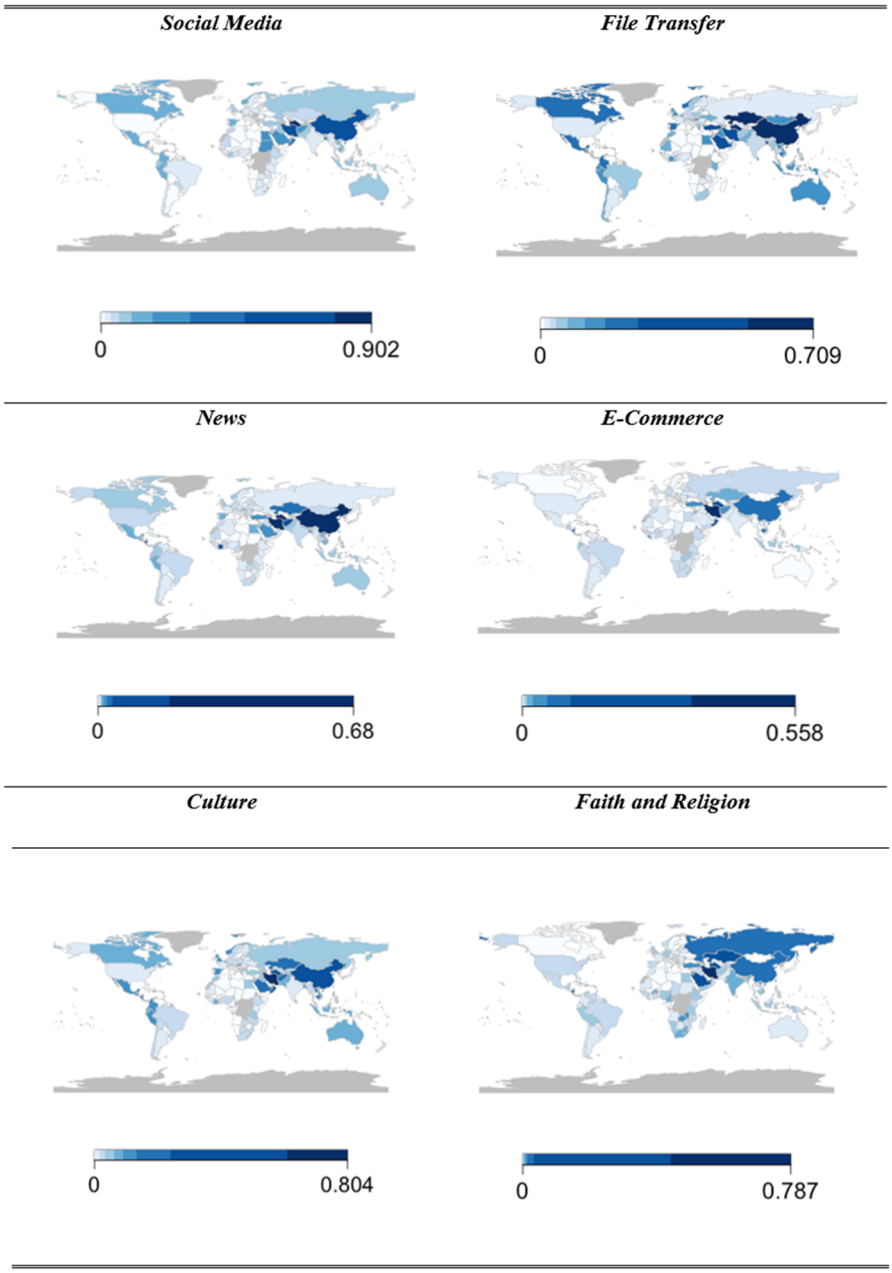

Figure 4. Intensity of blocking major foreign websites. Major websites (by traffic) are ranked by SimilarWeb: https://www.similarweb.com. Data on incidence of blocking is from Censored Planet Project: https://censoredplanet.org/.

D. Discussion: Cyberborders and Terrestrial Borders

Over a decade ago, Goldsmith and Wu observed that it was indeed possible for states to exert their territorial authority to border the internet. Not only is this possible, but it is a reenactment of states' ongoing struggle to maintain a sovereign identity in the face of global forces. Moreover, the concept of border orientation captures the underlying preference to engineer distinctiveness. Figure 5 summarizes the remarkably strong relationship between cyberborders on the one hand and border orientation on the other. To measure cyberborders, we created an additive index for each country from the three cyberborder policies described above (data localization, takedown requests, and website blocking). These values are denoted on the vertical axis. Border orientation is along the horizontal axis. It is a latent variable developed from physical bordering responses (walls, fences, border inspection stations, and police stations in border zones) that represents a state's commitment to controlling the penetration of its national border. The relationship is positive (correlation = 0.27) and extremely tight (p=.0018). The results suggest cyberborders spring from the same horizontal preference for jurisdictional distinctiveness and spatial control. States that have highly controlling border orientations toward the movement of goods and people also tend to erect more cyberborders that control the movement of data. This summary figure underscores the limitations of claims of cyber exceptionalism. It also suggests that the states have fought to preserve their sovereign identity and have indeed attempted to do so in the digital age as well.

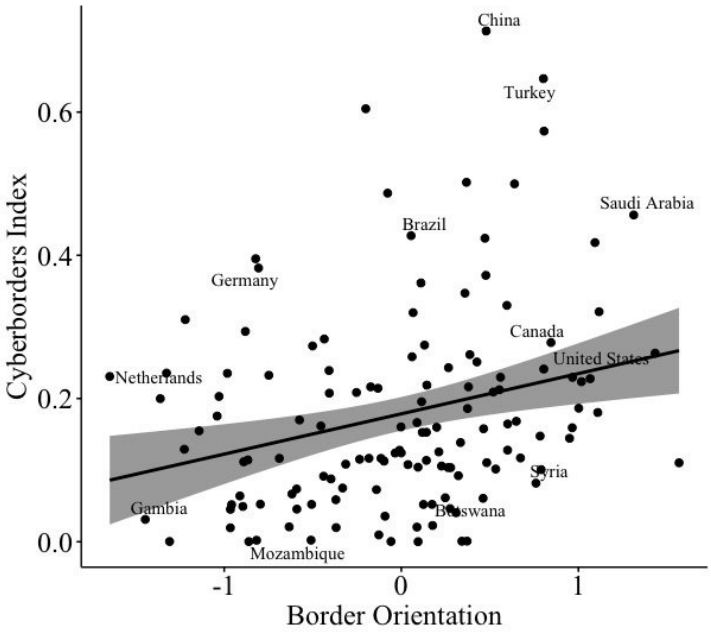

Figure 5. *The correlation between cyberborders and border orientation.* The cyberborder index is comprised of data localization laws, take-down requests, and website blocking. The border orientation score is a latent variable developed from border crossing structures, border walls and fences, and police stations in border zones to represent a state's commitment to the public, authoritative, and spatial display of

controlling cross border movement. The correlation between these two indexes is 0.27 (p=.0018).

CONCLUSION

Sovereignty in cyberspace has often been characterized as a unique concern. This Essay has reviewed cyber exceptionalism—paralleling other debates about the nature of state sovereignty in the face of globalization. We argue instead for a broader understanding of states' sovereign identity crises. States have been grappling with the limits of their own territorial control for decades. They have dealt with trade, human mobility, transnational crime and violence, and the challenges such cross-border movements pose for governability. Variance in sensitivities to jurisdictional distinctiveness in the face of these challenges can be captured by the concept of border orientation. To varying degrees, states respond to information flows by bordering. Such a move is not unique. Indeed, many bordering routines are a reprise of policies to shore up states' capacity to filter many kinds of transactions at their national borders.

Despite the anxieties produced by the information age and the attendant sovereign identity crisis, we suggest that states can and do border the internet in ways that are mirrored at their geographic borders in the physical world. We enumerated the various ways that states engage in highly territorial practices and rhetoric to maintain national distinctiveness and drive a wedge between foreign and domestic. Governments will continue to rely on geographic concepts to guide and direct policy in unfamiliar territories. Although the anxiety over managing mercurial flows, such as the internet, may vary by country and vacillate over time, we demonstrate that the states that have already taken strong stands to carve out jurisdictional distinctiveness are the same countries that take the strongest stands when emerging forms of globalization arise. Our research suggests that the sovereign identity crisis can be understood through the familiar concept and practice of bordering.

Policy implications abound from widening the analytical aperture from censorship to the lens of cyberborders. Practices to limit the movement of information are not isolated to only the most repressive jurisdictions. Democracies also have motivations to remove content, and sometimes for liberal reasons. Our study suggests the need to consider the diverse motivations across regime types for controlling cross-border information flows.

Internationally, our research speaks to robust global debates over the implications of internet fragmentation.[110] The phenomenon has been described as digitally bordered

110. *See* JONAH FORCE HILL, INTERNET FRAGMENTATION: HIGHLIGHTING THE MAJOR TECHNICAL, GOVERNANCE AND DIPLOMATIC CHALLENGES FOR U.S. POLICY MAKERS (2012), https://www.belfercenter.org/publication/internet-fragmentation-highlighting-major-technical-governance-and-diplomatic [https://perma.cc/XY8L-4GMT]; ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS (2013); Sérgio Alves Jr., Internet Governance 2.0.1.4: The Internet Balkanization Fragmentation (July 16, 2014), http://dx.doi.org/10.2139/ssrn.2466222.

"national Internets,"[111] the "balkanized Internet,"[112] and "splinternets"[113] to represent the same outcome: distinctive zones of digital content that arise through government actions. We explain the societal forces driving fragmentation that motivate the construction of online and offline walls: controlling foreign flows and, thereby, protecting jurisdictional distinctiveness. Since fragmentation comes at a price—connectivity—policymakers should continue to deliberate the meaning and appropriate responses to the construction of digital walls. Our research provides the tools to identify where and when these changes occur to motivate further work on the implications and appropriate policy responses to online borders.

111. WILLIAM J. DRAKE, VINTON G. CERF & WOLFGANG KLEINWÄCHTER, WORLD ECON. F., INTERNET FRAGMENTATION: AN OVERVIEW (2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [https://perma.cc/7A74-CFVK].

112. *See* Katherine Maher, *The New Westphalian Web*, FOREIGN POL'Y (Feb. 25, 2013), https://foreignpolicy.com/2013/02/25/the-new-westphalian-web/ [https://perma.cc/HGD7-8CRY]; Tim Maurer & Robert Morgus, *Stop Calling Decentralization of the Internet "Balkanization"*, SLATE (Feb. 19, 2014), https://slate.com/technology/2014/02/stop-calling-decentralization-of-the-internet-balkanization.html [https://perma.cc/7GM7-TSFW]; Bob Davis, *Rise of Nationalism Frays Global Ties*, WALL ST. J. (Apr. 28, 2008), http://online.wsj.com/article/SB120934738145948747.html [https://perma.cc/F7WV-EUTB] ("We're facing a step-by-step Balkanization of the global Internet . . . [i]t's becoming a series of national networks.").

113. *See* Grothaus, *supra* note 10.