Brooklyn Journal of International Law

Volume 46 | Issue 1 Article 1

12-31-2020

Data Governance and the Elasticity of Sovereignty

Roxana Vatanparast

DATA GOVERNANCE AND THE ELASTICITY OF SOVEREIGNTY

Roxana Vatanparast[*]

---

* Research Fellow, Program on Science, Technology and Society (STS Program), Harvard Kennedy School; formerly Visiting Researcher, Institute for Global Law & Policy (IGLP) at Harvard Law School; PhD, University of Turin; JD, UC Hastings College of the Law. A short version of this Article was presented at the European Society of International Law (ESIL) Conference in Athens, Greece in September 2019, and an earlier draft has been published as part of the 2019 ESIL Annual Conference Proceedings Working Paper Series. I would like to thank Alberto Oddenino, as well as my writing workshop group at the 2019 IGLP Scholars Workshop for insightful comments on a prior draft of this Article, and in particular Delphine Dogot, Richard Joyce, Mohammad Shahabuddin, and Hilton Simmet. I thank the excellent editors of the *Brooklyn Journal of International Law* for their helpful suggestions and edits. I would also like to express my gratitude to the IGLP, STS Program, and University of Turin for institutional support during the writing of this Article. All errors remain mine. Contact: roxanav41@gmail.com.

INTRODUCTION: THE MYTH OF TERRITORIAL SOVEREIGNTY

What might ancient Greek myths tell us about sovereignty? Paul Veyne's *Did the Greeks Believe in Their Myths?* highlights the role of imagination in constructing truths, and the possibility of belief in contradictory things.[1] As he notes, "[i]t is precisely because the mythical world is definitively other, inaccessible, different, and remarkable that the problem of its authenticity is suspended . . . ."[2]

Similarly, Yaron Ezrahi has highlighted the performative role of imagination in democratic politics.[3] In theorizing the performativity of political imaginaries, he says:

> Political imaginaries . . . refer to fictions, metaphors, ideas, images, or conceptions that acquire the power to regulate and shape political behavior and institutions in a particular society. [. . .] Although initially political fictions commonly suggest empirically baseless fabrications, some gain sufficient credibility and adherence to attain the status of performative imaginaries that produce behavior that, in turn, affirms them.[4]

Myth plays an especially significant role in both modern law's origins and in the reconciliation of its internal contradictions.[5] Myths, fictions, and imaginaries are particularly instructive in the case of sovereignty. Myth functions to transmit a useful teaching, "or a physical or theological doctrine hidden under the

---

1. *See generally* PAUL VEYNE, DID THE GREEKS BELIEVE IN THEIR MYTHS?: AN ESSAY ON THE CONSTITUTIVE IMAGINATION (Paula Wissing tran., 1988).

2. *Id.* at 20.

3. *See generally* YARON EZRAHI, IMAGINED DEMOCRACIES: NECESSARY POLITICAL FICTIONS (2015).

4. *Id.* at 3.

5. *See generally,* PETER FITZPATRICK, THE MYTHOLOGY OF MODERN LAW (1992).

veil of allegory, or the memory of events of past times."[6] Ernst Kantorowicz's reference to the symbolic "body politic" of the sovereign meeting the natural body of the king in the statement, "The king is dead. Long live the king."[7] is also instructive of the role of myth, metaphor, and political imaginaries in sense-making of political power and authority.[8]

What accounts for the continuing belief in the myth of sovereignty? Is sovereignty part of the political imaginary of international law?

Many scholars in the 1990s claimed that the power of the state and sovereignty were declining in the era of globalization, with some even proclaiming the "retreat of the state"[9] or the "death of sovereignty."[10] Today, in contrast, it seems that there is a move towards increasing sovereignty, such as in the areas of trade and migration, and in the context of populist movements.[11] This Article is an attempt to move beyond the oscillation between these two conceptualizations. The multiple forms that sovereignty takes[12] reveal what I term the "elasticity of sovereignty."

---

6. *Id.*

7. ERNST H. KANTOROWICZ, THE KING'S TWO BODIES: A STUDY IN MEDIEVAL POLITICAL THEOLOGY 7–16 (2016). According to Kantorowicz, the body politic refers to the "mystic body" of the king which was immortalized through the institution of the monarchy, and represents the relationship between a king and his subjects. *See id.* at 15–16.

8. On the mystical and demonological origins of the figure of the *dominus mundi* in the imagination of legal and political theorists discussing sovereignty, *see* PIER GIUSEPPE MONATERI, DOMINUS MUNDI: POLITICAL SUBLIME AND THE WORLD ORDER (2018).

9. *See generally* SUSAN STRANGE, THE RETREAT OF THE STATE: THE DIFFUSION OF POWER IN THE WORLD ECONOMY (1996).

10. On this as an exaggerated claim, *see* James Crawford, *Sovereignty as a Legal Value in* THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW 117, 132 (James Crawford & Martti Koskenniemi eds., 2012).

11. Janne E. Nijman & Wouter G. Werner, *Populism and International Law: What Backlash and Which Rubicon?*, 49 *in* NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 2018: POPULISM AND INTERNATIONAL LAW 3, 6–10 (Janne E. Nijman & Wouter G. Werner eds., 2019).

12. Regarding types of sovereignty, *see* STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY (1999) (distinguishing between international legal sovereignty, Westphalian sovereignty, domestic sovereignty, and interdependence sovereignty). On multiple, overlapping, and competing sovereignties, *see also* Shalini Randeria, *The State of Globalization: Legal Plurality, Overlapping Sovereignties and Ambiguous Alliances between Civil Society and the Cunning State in India*, 24 THEORY, CULTURE & SOC'Y 1, 1–33 (2007); RICHARD JOYCE, COMPETING SOVEREIGNTIES (2012); and Gerry Simpson, *Something to do with*

Theorizing sovereignty as elastic might encapsulate its multiple meanings,[13] the various ways in which it changes over time and in different contexts, and account for its internal contradictions as a concept. At the same time, this elasticity leaves room for sovereignty as a myth to be continually reshaped and reimagined by a variety of actors. It is therefore no surprise that alternative forms of authority (sovereign, quasi-sovereign, or otherwise) should arise in the context of this elasticity, especially in spaces which do not fit neatly within the territorial framework underlying much of international law's conceptualization of sovereignty. According to Martti Koskenniemi, sovereignty has no fixed content, subjecting it to a variety of meanings and uses.[14] The controversies, contestations, and contingencies around the concept of sovereignty itself,[15] along with its unsettled status, are precisely what give sovereignty its meaning and durability as an expert vocabulary. As David Kennedy says, "for many forms of global expertise: the less decisive, determinative or univocal an expert vocabulary, the more prevalent it becomes."[16]

This Article will discuss how regulations of cross-border transfers of data attempt to exercise territorial sovereignty and jurisdiction over what some call a "post-territorial"[17] phenomenon. Data both illustrates and challenges the concept of territorial sovereignty in international law, entailing a different way of mapping and theorizing global power and authority. Simultaneously local, national, and global data enables new geographies of private and public power untethered to traditional conceptions of territoriality. Yet regulation and policy on data privacy and cross-border data transfers still attempt to link digital data to territorial sovereignty and jurisdiction. By comparing the regulatory approaches of China, the European Union (EU), and the

---

States, *in* THE OXFORD HANDBOOK OF THE THEORY OF INTERNATIONAL LAW 580 (Anne Orford & Florian Hoffmann eds., 2016).

13. On its multiple meanings in international law, *see* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 448–49 (8th ed. 2012).

14. Martti Koskenniemi, *What Use for Sovereignty Today?*, 1 ASIAN J. INT'L L. 61, 61–70 (2011).

15. JENS BARTELSON, A GENEALOGY OF SOVEREIGNTY 2 (1995).

16. DAVID KENNEDY, A WORLD OF STRUGGLE: HOW POWER, LAW, AND EXPERTISE SHAPE GLOBAL POLITICAL ECONOMY 293 (2018).

17. Paul De Hert & Johannes Thumfart, *The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies*, 5 (BRUSSELS PRIVACY HUB, Working Paper No. 11, 2018).

United States (US), this Article shows that these approaches reflect a dual logic with regard to territoriality and data, at once moving away from territoriality, while at the same time "re-territorializing" by linking regulations to the location of users, data collectors, or data infrastructure. This flexible approach towards data governance across borders shows that territorial sovereignty is often repurposed, which is something that is not unique to data governance.[18]

Digital data reveals that sovereignty is elastic and sometimes contradictory, it is multiple in the forms in which we see it enacted, and the power and authority it represents are capable of being enacted by a variety of human and non-human agents.[19] In other words, this theorization decenters the state as the central locus of power and authority and allows us to map exercises of power and authority beyond the restrictive territorial state-based models prevalent in international law, in a way that is more in tune with how global political economy functions today. At the same time, however, this Article does not propose doing away with the state entirely. Moreover, this Article argues against conceptualizing data as something exceptional. Rather, it will demonstrate the elasticity of sovereignty has long permitted states and powerful global actors to territorialize people, things, and processes that were not strictly within their territorial borders.

The repurposing of sovereignty in the digital data context shows some of the broader ways in which states and regulatory authorities adapt their sovereign authority through assertions of jurisdiction,[20] exemplifying yet another creative reimagining of the elasticity of sovereignty.[21] These exercises in

---

18. On territory itself being "a process, made and remade, shaped and shaping, active and reactive," *see* STUART ELDEN, THE BIRTH OF TERRITORY 17 (2013); on "cyberspace" being "subjected to continuous processes of deterritorialization and reterritorialization," *see* Daniel Lambach, *The Territorialization of Cyberspace*, 22 INT'L STUD. REV. 3, 25 (2019).

19. BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY 164 (2005).

20. Sundhya Pahuja & Shaun McVeigh, *Rival Jurisdictions: The Promise and Loss of Sovereignty*, *in* AFTER SOVEREIGNTY: ON THE QUESTION OF POLITICAL BEGINNINGS 99 (George Pavlich & Charles Barbour eds., 2010).

21. Elasticity as a quality of sovereignty has also been described by previous scholars in other contexts, such as Hans Aufricht, *On Relative Sovereignty*, 30 CORNELL L.Q. 137, 147 (1944); Hikaru Yamashita, *Fighting Terrorism and*

reimagination are significant when we consider their distributional effects and how they allocate decision-making power and authority, as well as how they constitute and shape political communities. Digital data has become intertwined with a variety of technical practices that are involved in multiple and overlapping exercises of jurisdiction, each with their own set of normative commitments that can come into conflict with the others.[22] Moreover, they also reveal that where law and sovereignty are elastic, exercises of authority, governance, and decision-making become functions of power.[23] Power here is understood to mean "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances."[24] As these exercises of power increasingly take on qualities of management within depoliticized "global expert regimes," they require novel ways of re-politicizing social problems and challenging those exercises of power.[25]

I. TOWARD A THEORY OF SOVEREIGNTY

This section will discuss several influential theories of sovereignty in political and international legal thought and some of their critiques. It will then discuss the decoupling of sovereignty and territory, and arguments which have challenged traditional thinking on sovereignty as necessarily tied to territory.

A. Mapping the Debates and Critiques

Much has changed since Jean Bodin wrote his oft-cited quote on sovereignty, where he describes it as "the absolute and perpetual power of a commonwealth, which the Latins call *maiestas*; the Greeks *akra exousia*, *kurion arche*, and *kurion politeuma*; and the Italians *segnioria*, a word they use for private

---

Fighting Humanitarian Emergencies: Two Approaches to 'Elastic' Sovereignty and International Order, 18 CAMBRIDGE REV. INT'L AFF. 105, 112, 115 (2005).

22. Fleur Johns & Caroline Compton, *Data jurisdictions and rival regimes of algorithmic regulation*, REG. & GOVERNANCE 1, 1–4 (2019).

23. Katharina Pistor, *A Legal Theory of Finance*, 41 J. COMP. ECON. 315, 323 (2013). "Where law is elastic decisions are not predetermined by legal rules but left to the discretion of 'power wielders.' Power can thus be defined as the differential relation to law. Where law is elastic power becomes salient." *Id.* (internal citations omitted).

24. Michael Barnett & Raymond Duvall, *Power in International Politics*, 59 INT'L ORG. 39, 42 (2005).

25. Koskenniemi, *supra* note 14, at 68.

persons as well as for those who have full control of the state, while the Hebrews call it *tomech shévet*—that is, the highest power of command."[26] The debate on sovereignty is a rich and complex one, both in political and legal theory, with little agreement on how to define it or what it really constitutes. As the traditional theories and conceptions of sovereignty are increasingly being challenged by contemporary developments, transformations, and changes in world relations, new conceptions are now being developed to cope with those changes and to reflect new understandings of the world, politics, and the law.

Some scholars attribute the origins of modern notions of state sovereignty to the Peace of Westphalia (1648), or the treaties entered into in the aftermath of the Thirty Years' War.[27] Yet others argue that the idea that the concept of sovereignty should be territorially bounded did not arise during the Peace of Westphalia, but much later in the nineteenth century.[28] For example, Christopher Rossi argues that the Peace of Westphalia "did not . . . contain any recognizably modern notion of territorially bounded sovereignty," but rather that this connection arose later.[29] What was missing was a conception of the state that could connect sovereignty and territoriality. Once states internalized a notion of autonomy, they could bind the two concepts together.[30]

Moreover, the idea that sovereignty could be divisible internally, but indivisible externally, was another development that led to sovereignty becoming a quality associated with the state.[31] That association brought the notion of territoriality into close relation with the idea of reciprocal sovereignty and ideas of noninterference that were derived from property law concepts of trespassing.[32] Scholars have drawn parallels to the exercise of sovereign power and authority (*imperium*) and the embedded ideas of property rights (*dominium*), derived from principles of

---

26. JEAN BODIN, ON SOVEREIGNTY: FOUR CHAPTERS FROM THE SIX BOOKS OF THE COMMONWEALTH 1 (Julian H. Franklin ed., & tran., 13th ed. 2010).

27. Leo Gross, *The Peace of Westphalia, 1648-1948*, 42 AM. J. INT'L L. 20, 21 (1948).

28. Andreas Osiander, *Sovereignty, International Relations, and the Westphalian Myth*, 55 INT'L ORG. 251, 281 (2001); ELDEN, *supra* note 18, at 310.

29. CHRISTOPHER R. ROSSI, SOVEREIGNTY AND TERRITORIAL TEMPTATION: THE GROTIAN TENDENCY 17 (2017).

30. *Id.* at 18.

31. *Id.*

32. *Id.*

Roman law.[33] Other comparisons between contract law, the state, and conceptions of sovereignty derive from the idea of the Hobbesian social contract,[34] but also from the etymology of the word state itself, which is something between contract (*estate*) and status (*stato*).[35]

In the twentieth century, one of the most influential theories of the sovereign derived from Carl Schmitt, who claimed that "the sovereign is he who decides on the state of exception,"[36] making decision-making on the "state of exception" a central basis for sovereignty.[37] Yet Schmitt's theory was premised upon a centralized authority with the power to decide. Building upon Schmitt's theory, Agamben's critique of sovereignty premised on the state of exception also reinforces the role of a centralized sovereign decision-making authority.[38]

In contrast to Hobbes', Schmitt's, and Agamben's accounts of a centralized sovereign authority, Foucault's critique of sovereignty called for imagining its multiplicity in forms, forces, spaces, institutions, and populations over and through which it was exercised.[39] Yet, as other scholars have noted, he still assumed a fixity to population and territory in relation to sovereign power—which does not fit with the ways sovereign power has been exercised both historically and today[40]—and held a Eurocentric view of sovereignty.[41]

---

33. *Id.* at 19. *See also* Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8, 8 (1927).

34. THOMAS HOBBES, LEVIATHAN 162 (1982).

35. ROSSI, *supra* note 29, at 17.

36. CARL SCHMITT, POLITICAL THEOLOGY: FOUR CHAPTERS ON THE CONCEPT OF SOVEREIGNTY 5 (George Schwab trans., 1985).

37. *See id.* at 7. A state of exception, according to Schmitt, is a state in which the law can be suspended and the sovereign can take actions that would otherwise be considered illegal or extralegal, but which are justified by appeals to necessity in emergency or exceptional situations. *Id.*

38. GIORGIO AGAMBEN, HOMO SACER: SOVEREIGN POWER AND BARE LIFE 16 (Daniel Heller-Roazen trans., 1998).

39. MICHEL FOUCAULT, "SOCIETY MUST BE DEFENDED": LECTURES AT THE COLLÈGE DE FRANCE, 1975-1976 265–67 (Mauro Bertani, Alessandro Fontana, François Ewald eds., David Macey trans., 2003).

40. Sheila Jasanoff, *Subjects of reason: goods, markets and competing imaginaries of global governance*, 4 LONDON REV. INT'L L. 361, 364 (2016).

41. Andrew W. Neal, *Cutting off the King's Head: Foucault's* Society Must Be Defended *and the Problem of Sovereignty*, 29 ALTERNATIVES: GLOBAL, LOCAL, POL. 373, 392 (2004).

From the perspective of international law, unequal sovereignty played a significant role in colonial and imperial endeavors. Unequal sovereignty was displayed most prominently in the drawing of maps and state territorial lines by European powers, as witnessed at the 1885 Berlin Conference, the occupation of *terra nullius*, and by the denial of sovereignty to non-European peoples.[42] The principle of sovereign equality of states masked the states' factual inequality and hierarchy, and became a status that marked the difference between the "civilized" and the "uncivilized."[43]

Post-colonial critiques of sovereignty question the usefulness of the concept altogether in light of the diffusion and fragmentation of power, and the transformations in the global order that have not only deterritorialized sovereignty but have also resulted in trade regimes and cross-border flows that challenge the fundamental role of the nation-state as previously conceptualized.[44] Other critiques and theorizations of sovereignty as having multiple meanings and subject to fluctuations over time and in different contexts have retained the centrality of the state in their theorizations.[45] Other theorists who have considered how technology is used as a tool in exercises of sovereignty presume that technology is replacing law and sovereignty.[46] While these critiques offer highly useful perspectives in rethinking sovereignty, the aim here is to move beyond the binary of territoriality and extraterritoriality and to highlight the mutual interaction between technology and shifting conceptualizations of sovereignty.

---

42. *See generally* ANTONY ANGHIE, IMPERIALISM, SOVEREIGNTY AND THE MAKING OF INTERNATIONAL LAW (2005); ANDREW FITZMAURICE, SOVEREIGNTY, PROPERTY AND EMPIRE, 1500-2000 (2014); JOHN AGNEW, GLOBALIZATION AND SOVEREIGNTY: BEYOND THE TERRITORIAL TRAP (2d ed. 2017).

43. ANGHIE, *supra* note 42; MARTTI KOSKENNIEMI, THE GENTLE CIVILIZER OF NATIONS: THE RISE AND FALL OF INTERNATIONAL LAW 1870–1960 98–178 (2001).

44. Brenna Bhandar, *The Conceit of Sovereignty: Towards Post-Colonial Technique*, *in* STORIED COMMUNITIES: NARRATIVES OF CONTACT AND ARRIVAL IN CONSTITUTING POLITICAL COMMUNITY 68, 68–69 (Hester Lessard, Rebecca Johnson & Jeremy Webber eds., 2010).

45. STEPHEN D. KRASNER, SOVEREIGNTY: ORGANIZED HYPOCRISY 9 (1999); BARTELSON, *supra* note 15, at 19.

46. *See, e.g.,* BENJAMIN H. BRATTON, THE STACK: ON SOFTWARE AND SOVEREIGNTY (2016); TUNG-HUI HU, A PREHISTORY OF THE CLOUD (2016).

B. Decoupling Sovereignty and Territory

Long before scholars of globalization in international relations and international law were discussing the decoupling of sovereignty and authority from territory starting around the 1990s, Carl Schmitt described how the postwar period was marked by a move away from the Eurocentric, Westphalian spatial order that had existed until the twentieth century.[47]

In more recent decades, international relations and international law scholars have been increasingly discussing globalization's effects on the diffusion of normative orders, authority, and rulemaking with global effects.[48] These derive from a variety of institutions and actors that go beyond the traditional idea of authority and law as solely originating from state sovereigns exercising independent, exclusive control over territory.[49]

The decoupling of the concept of sovereignty from territoriality and territorially enclosed borders is not new, despite many accounts to the contrary in the context of globalization.[50] John Agnew, for example, criticizes the idea that territorial sovereignty and globalization are either/or binaries. In Agnew's description, "the dominant image of globalization is the replacement of a presumably territorialized world by one of networks and flows that

47. CARL SCHMITT, THE NOMOS OF THE EARTH IN THE INTERNATIONAL LAW OF JUS PUBLICUM EUROPAEUM 351–53 (G. L. Ulmen tran., 2006).

48. *See, e.g.,* OUR GLOBAL NEIGHBOURHOOD: THE REPORT OF THE COMMISSION ON GLOBAL GOVERNANCE 2 (2015); Benedict Kingsbury, Nico Krisch & Richard B. Stewart, *The Emergence of Global Administrative Law*, 68 L. & CONTEMP. PROBS. 15, 15 (2005); Peer Zumbansen, *Defining the Space of Transnational Law: Legal Theory, Global Governance, and Legal Pluralism*, 21.2 TRANSNAT'L L. & CONTEMP. PROBS. 305, 305–36 (2012); *See generally* PRIVATE INTERNATIONAL LAW AND GLOBAL GOVERNANCE (Horatia Muir Watt & Diego P. Fernández Arroyo eds., 2014).

49. Several international law cases and advisory opinions uphold the principle of sovereignty as traditionally understood in customary international law as the exclusive, independent right to exercise authority over a territory. *See, e.g.,* Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928), where the court held that sovereignty corresponds to independence between states; Customs Regime Between Germany and Austria, Advisory Opinion, 1931 P.C.I.J. (ser. A/B) No. 4, at 12 (Sept. 5), where the court held that sovereignty is the exercise of the "sole right of decision in all matters economic, political, financial or other"; Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27), where the court upheld a state's territorial sovereignty and the customary international law norm of non-intervention into another state.

50. AGNEW, *supra* note 42.

know no borders other than those that define the earth as such."[51] Agnew's theory is one of multiple sovereignties, where sovereignty is conceived as not necessarily coupled with the state or territoriality. Such a broad conception can better account for dynamics of global power[52] and avoid assuming state-territoriality as the central locus of power—what he terms the "territorial trap."[53]

Moreover, as Nikolas Rajkovic argues, modern cartography served as a medium that dominated how spaces of authority have been conceptualized in international law.[54] Today, however, "increasingly non-territorialized configurations of persons, goods, threats, harms and wealth provoke doubt over the extent to which geographic reality remains by nature, and not artifice, territorial."[55] Despite this, he argues against the idea of deterritorialization, or the teleological end of territory, as commonly theorized.[56] Instead, he uses the term "reterritorialization" to reconceptualize space in international law, which acknowledges "how territory has never been constituted by an absolute and fixed materiality, but more accurately involving an evolving assemblage and materialization of things, actors and ideas . . . territorial boundaries have been always, to varying degrees, in temporal flux."[57]

II. DATA'S CHALLENGE TO TERRITORIALITY

This section will outline some of the challenges data raises to traditional notions of territoriality in international law. It will do so by first outlining the territoriality principle in international law, and then it will discuss some of the debates among legal scholars regarding the unique challenges that data raises to that principle.

---

51. *Id.* at Preface.

52. *Id.* at 30.

53. *Id.* at 30–31. The "territorial trap," according to Agnew, is the assumption of "an essential state-territoriality to the workings of power." *Id.*

54. Nikolas M. Rajkovic, *The Visual Conquest of International Law: Brute Boundaries, the Map, and the Legacy of Cartogenesis*, 31 LEIDEN J. INT'L L. 267, 267–88 (2018).

55. *Id.* at 268.

56. *Id.* at 273.

57. *Id.* at 275.

A. The Territoriality Principle

The principle of territoriality derives from the seventeenth century and has since become the primary basis for the assertion of jurisdiction in international law.[58] The territoriality doctrine under international law typically attributes to states plenary jurisdiction over all matters that fall within their territorial sovereignty.[59]

One of the foundational cases in international law regarding jurisdiction and the territoriality principle is *The Case of the S.S. "Lotus" (France v. Turkey)*.[60] Brought before the Permanent Court of International Justice (PCIJ), the dispute concerned whether Turkey could exercise criminal jurisdiction over a French national for a collision that occurred between a Turkish ship and a French ship on the high seas. In its decision, the PCIJ stated:

> Now the first and foremost restriction imposed by international law upon a State is that . . . it may not exercise its power in any form in the territory of another State . . . It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of acts which have taken place abroad . . . Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion.[61]

According to this reasoning, the PCIJ permitted the exercise of extraterritorial prescriptive jurisdiction in this case, as there was no rule prohibiting it and it did not involve enforcement in another state's territory.

The permissive principle of jurisdiction outside of a prohibitive rule to the contrary seems to be a principle that states still rely upon in practice.[62] At the same time, however, territorial

---

58. CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 50 (2015).

59. Bruno Simma & Andreas Th. Müller, *Exercise and limits of jurisdiction*, *in* THE CAMBRIDGE COMPANION TO INTERNATIONAL LAW, 137–38 (James Crawford & Martti Koskenniemi eds., 2012).

60. S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

61. *Id.* at ¶ 46.

62. RYNGAERT, *supra* note 58, at 34.

jurisdiction remains the customary international law norm,[63] with some exceptions. Nevertheless, the locus of conduct is considered central to the concept of territorial jurisdiction under international law and can have a variety of implications depending on *where* a certain act is deemed to be conducted. This is complicated by acts that stem from multiple places or those that have effects in places other than where they originated. As will be discussed, these examples are particularly evident in the context of cyberspace and data, which challenge the traditional spatial conceptions of international law based on territorial nation-states.

One way in which international law attempts to address this complication is through the "effects doctrine." Extraterritorial jurisdiction refers to the ability "to exercise jurisdiction over persons abroad (even non-nationals) for acts occurring abroad, which were intended to have, and indeed have, significant harmful [economic] effects within the territory asserting jurisdiction."[64] Generally, if the conduct or its effect occurs within a state's territory, a state can exercise subjective or objective territorial jurisdiction, respectively.[65] The effects doctrine is one type of objective territorial jurisdiction in which the intention to produce economic effects in a state's territory is deemed sufficient for that state to exercise jurisdiction.[66]

While not all states agree with the effects doctrine, which originated in US antitrust law, EU countries are increasingly exercising this type of jurisdiction.[67] In practice, states have interpreted the effects doctrine more broadly than just the purely economic context. This is evident in the context of regulation of data processing in the General Data Protection Regulation 2016/679 (GDPR), as will be discussed, where both regulatory authorities and the Court of Justice of the European Union (CJEU) have adopted a variation of this broad approach, which provides the basis for the exercise of extraterritorial jurisdiction.[68] The complexities and the interconnectedness of the global economy and technology provide ample bases for the effects doctrine, but interpreting it too broadly risks "too much" jurisdiction, where

63. *Id.* at 35.

64. ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 74 (1995).

65. Simma and Müller, *supra* note 59, at 140.

66. *Id.*

67. *Id.*

68. As further discussed herein. *See infra* Section III.B.

multiple states will assert jurisdiction or promulgate competing or conflicting regulations over the same conduct, creating a positive conflict of jurisdiction.[69]

Moreover, while states are expanding their extraterritorial jurisdiction in some areas, such as environmental law, sanctions laws, and anticorruption legislation, they are limiting it in other areas, such as criminal and tort law.[70] As shall be demonstrated, there is a tendency toward extraterritorial reach—whether explicitly intended as such, or having such effects—in the context of regulations on data protection and cross-border data transfers.

B. Data & Territoriality

According to Jennifer Daskal, data is intangible, divisible, mobile, and interconnected.[71] It is often fragmented, copied, with different component parts stored in different places, constantly being dissembled and reassembled (at times by algorithms), and moved around to different locations without the knowledge of users.[72] Cloud computing and data depend on borderless networks. Multiple jurisdictions often necessarily come into play with regard to data transfers since different components of data are often stored in different places and can be accessed from multiple places at once. Given the mobile and divisible qualities of data, basing territoriality and jurisdiction determinations on the location of data can be arbitrary and complex.[73] In the words of Kristen Eichensehr, "[t]he problem is not that data is located *nowhere*, but that it may be located *anywhere*, and at least parts of it may be located nearly *everywhere*."[74]

---

69. Simma and Müller, *supra* note 59 at 141.

70. This can be seen in the tort context, for example, in the limitation of the extraterritorial applicability of the Alien Tort Statute in recent United States Supreme Court litigation, where the Court found that the claims did not sufficiently "touch and concern the territory of the United States" where the plaintiffs were Nigerian citizens complaining of conduct committed by Dutch, Nigerian, and British corporations in Nigeria. *See* Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 117 (2013).

71. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 366–76 (2015).

72. *Id.* at 366–67.

73. *Id.* at 369.

74. Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. 145, 145 (2017).

Digital data's unique relationship with territory is illustrated by cross-border data flows, or the movement of data across borders.[75] Data is often stored in a different location from the user.[76] Users typically have no control over where their data is stored and often times lack any knowledge of where it is located or which jurisdictions' laws might be governing it.[77]

Moreover, due to the interconnectedness of global communications today, the data of a US person might be intermingled with a non-US person's data. Data can be intermingled, even unintentionally, to such an extent that data can be "incidentally" collected on a number of people at once.[78] This creates challenges in determining the location of the data, and regulating users on the basis of their location or identity.[79] Finally, location independence between the data and the government agents accessing the data can occur in such a way that even if a state is accessing data on a subject in another state for investigatory purposes, there might not be a violation of territorial sovereignty of the other state.[80] While other legal mechanisms, such as standard contractual clauses and mutual legal assistance treaties (MLATs), are prominent in the governance of cross-border data transfers, they do not address underlying questions around the mobility and divisibility of digital data that often justify broad assertions of jurisdiction.[81]

Some scholars refer to data and cloud computing as "post-territorial."[82] In other words, since data is distributed so widely, "it does not make sense to think of data as something that occupies an identifiable territory at all."[83] Nevertheless, since its movement and storage depends upon the material infrastructures of the internet, such as data servers, it does not make sense to refer

---

75. Some scholars argue against "cloud data exceptionalism." *See* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 729 (2016). For a critique of Woods' arguments, *see* RADIM POLCAK & DAN JERKER B. SVANTESSON, INFORMATION SOVEREIGNTY: DATA PRIVACY, SOVEREIGN POWERS AND THE RULE OF LAW 1, 54–57 (2017).

76. Daskal, *supra* note 71, at 373.

77. *Id.* at 378.

78. *Id.* at 379.

79. *Id.*

80. *Id.*

81. *Id.* at 393–94.

82. Hert & Thumfart, *supra* note 17, at 10.

83. *Id.*

to it as "non-territorial" either.[84] This creates a complex relationship between data and territory that does not fit neatly within categorizations of territoriality, extraterritoriality, or non-territoriality.

There are a number of options that are available in answering the question of where to locate data for legal and jurisdictional purposes. Is it located where it is stored? Is it located where it is accessed? Is it located where the data controller or processor is established? Or is it located where the data-generating subject is located and emits data?

Where to locate data for jurisdictional purposes is a central question that has arisen in recent cases[85] and for which recent proposals and regulations aim to provide clearer answers. As will be discussed next, recent regulations on data flows illustrate different jurisdictions' approaches to the link between data and territory. While they differ in quite a number of regards, they also have similarities in their tendencies toward extraterritoriality and reterritorialization.

III. Comparative Analysis of Data Transfer Regulations[86]

This section analyzes the regulatory frameworks around data transfers in China, the EU, and the US with regard to their approaches to territoriality. Each jurisdiction has its own ways of tying data to its territory, by linking their laws on data transfers to data infrastructure, data subjects, or data controllers, thereby reterritorializing data. On the other hand, each jurisdiction also has extraterritorial dimensions, as will be shown.

A. China

Cyberspace sovereignty and data sovereignty are qualities that are attributable to the Chinese approach toward data transfer regulations. Moving away from the sectoral approach toward privacy regulations, the Cybersecurity Law of 2016 has created

---

84. *Id.*

85. United States v. Microsoft Corp., 138 U.S. 1186, 1187 (2018).

86. As the laws, regulations, and policies around cross-border data transfers are likely to change frequently in the coming years, this Article focuses on the policies current at the time of writing (June 2019), but the overall argument should not change, as we can see the dual dynamic of reterritorialization and extraterritoriality tends to be consistent. Thus, the broader argument about the elasticity of sovereignty and the role of data and technological processes should remain relevant even in the case of regulatory changes taking place.

a broad framework under which data privacy protections fall and which applies to almost all public and private entities.[87] These provisions include data localization requirements for personal information and "important data."[88] Data localization in China is driven more by national security concerns than the protection of personal information and the rights of data subjects.[89] According to one of the drafters of the Cybersecurity Law, "the cross-border data transfer rules address the threats of data security and national security in the era of big data—massive amounts of data are controlled by the private sector, the accuracy and value of which may even surpass government data, and hostile foreign forces may use such data to subvert the Chinese government, launch cyber-attacks and endanger Chinese national security."[90]

Any data deemed to be related to state secrets is strictly protected under data transfer regulations.[91] State secrets can refer to anything relating to national security or interests, and the State Secrets Bureau makes determinations as to what constitutes a state secret.[92] Such determinations can even be made retroactively.[93] Location and mapping data, for example, can be considered state secrets if they contain specific information on certain facilities or a certain level of precision.[94] The transfer of state secrets out of China is prohibited.[95] With the exception of these state secrets regulations, data transfer regulations implemented prior to the Cybersecurity Law on matters such as the transfer of human genetic data, financial data, and demographic health data were rarely implemented, and thus had limited effects.[96]

---

87. Kemeng Cai, *Jurisdictional Report: People's Republic of China*, *in* REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 62, 64 (Asian Business Law Institute ed., 2018).

88. *Id.*

89. *Id.* at 65.

90. *Id.* at 91.

91. *Id.* at 65–66.

92. *Id.* at 66.

93. *Id.*

94. *Id.* at 71. Even if not considered state secrets, mapping data must be stored on data servers in China. *See id.* at 72.

95. *Id.* at 67.

96. *Id.* at 72.

The data localization requirements of the Cybersecurity Law apply to critical information infrastructure operators (CIIOs).[97] The Cybersecurity Law provides that personal information and data collected by CIIOs must be stored within China, with limited exceptions provided for the transfer of such data outside of the country.[98] In 2017, the Cybersecurity Administration of China (CAC) issued draft Measures for Security Assessment of the Cross-Border Transfer of Personal Information and Important Data (Draft Data Export Measures). The Draft Data Export Measures extend the data localization requirements to all network operators, not solely to CIIOs as set out in the Cybersecurity Law.[99] Under these measures, personal information and "important data"[100] collected or generated by network operators while operating in China must be stored in China.[101] Moreover, network operators must provide express notice and obtain consent of the individuals whose data is concerned before exporting personal data.[102] The exportation of personal data is not permitted if national security interests are implicated.[103]

In 2017, the draft of the Information Security Technology Guidelines for Cross-Border Data Transfer Security Assessment was also released (Draft Data Export Guidelines). While nonbinding, the Draft Data Export Guidelines provide guidance on assessment of data exports. These Guidelines define a "data export" as

> (a) personal information and important data provided to any entity within China who is not subject to the jurisdiction of China or not registered in China; (b) data not

97. According to Cai, "CIIOs are a subset of network operators subject to heightened cybersecurity requirements under the Cybersecurity Law. The Cybersecurity Law vaguely defines critical information infrastructures ("CII") as information infrastructures in 'public communication and information services, energy, traffic and transportation, irrigation, finance, public service, e-government and other key industries and sectors', as well as other information infrastructures, 'the damage, malfunction and data leakage of which may seriously endanger national security, national welfare, people's livelihood, and public interest' . . . ." *See id.* at 75.

98. *Id.* at 74 (citing Article 37 of the Cybersecurity Law).

99. *Id.* at 77.

100. This is defined as "data closely related to national security, economic development and public interests." *See Id.* at 78.

101. *Id.* at 77.

102. *Id.* at 78.

103. *Id.* at 79.

> transferred or stored outside China are accessed and viewed by overseas institutions, organisations and individuals (except for public information and webpage visits); and (c) a company group exports its internal data which involve personal information and important data collected and generated in the course of its operations within China.[104]

The "export of personal information and important data in transit in China" and the "export of personal information and important data not collected or generated in the course of operations in China but being processed in China for outsourcing purposes," however, are not considered "data exports."[105] Under this approach, where the data is generated and collected are determining factors.

In June 2019, China released draft measures for cross-border transfers of data called the Personal Information Outbound Transfer Security Assessment Measures (2019 Draft Measures).[106] The 2019 Draft Measures apply to network operators who collect personal information in the course of operations within mainland China.[107] These measures require that operators conduct security assessments to determine whether transfers of personal data outside of China would affect national security or harm public interest.[108] If operators find such effect, or find that personal information is difficult to protect, then data cannot leave the country.[109] Network operators must report their findings to the provincial-level cybersecurity and informatization department prior to the outbound transfer of personal data.[110] Organizations outside of China, as long as they collect personal information of users in China, must comply with the 2019 Draft Measures either through local representatives or local organizations.[111]

---

104. *Id.* at 82–83.
105. *Id.* at 83.
106. Cindy L, Qiheng Chen, Mingli Shi & Kevin Neville, *Translation: New Draft Rules on Cross-Border Transfer of Personal Information Out of China*, NEW AM. (June 13, 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.
107. *Id.* art. 2.
108. *Id.*
109. *Id.*
110. *Id.* art. 3.
111. *Id.* art. 20.

Although there have not been any formal enforcement actions on data localization yet, some companies have started moving their data gathered on Chinese citizens to data servers in China.[112] Foreign technology companies, including Microsoft, IBM, Apple, and Amazon, must work with Chinese-owned data centers (either privately-owned or government-owned), since foreign companies are not permitted to license data centers.[113] This illustrates some of the *de facto* extraterritorial effects of the regulations.

China's approach to governance of cross-border data flows reflects its broader approach to the regulation of content and information over the internet, some of which are filtered or blocked within its borders.[114] While it does this, the Chinese government is also investing heavily in building infrastructure within its borders and in expanding communications infrastructure around the world as part of its Digital Silk Road initiative.[115] This not only creates a Chinese-centric transnational network infrastructure, but also expands China's political and economic influence globally.[116] These policies—the former aimed at localization within its borders and the latter aimed at expansion of its transnational network infrastructure—might explain the move to reterritorialize and at the same time have extraterritorial reach. More broadly, these initiatives point to China seeking to "both to control information flows for political reasons and to further China's status as a rising global economic powerhouse . . . ."[117]

B. European Union

This section will discuss two examples of the EU's approach toward governance of data protection and cross-border data transfers. It will first discuss the GDPR and then the proposed

---

112. Cai, *supra* note 87, at 94.

113. Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, HENRY M. JACKSON SCH. INT'L STUD. (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

114. Jonathan Zittrain & Benjamin Edelman, *Internet Filtering in China*, 7 IEEE INTERNET COMPUTING 70, 70 (2003).

115. *See generally* Hong Shen, *Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative*, 12 INT'L J. COMMC'N 2683, 2683–701 (2018).

116. *Id.*

117. JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 216 (2019).

E-evidence rules, illustrating the dynamics of extraterritoriality and reterritorialization of data.

1. GDPR

The GDPR was passed by the EU Parliament on April 27, 2016 and went into effect on May 25, 2018.[118] The EU Parliament intended GDPR to replace the Data Protection Directive 95/46/EC (DPD) and to: harmonize regulation of data privacy in the EU; protect EU citizens' privacy rights; and change the way organizations and companies treat data privacy.[119] The GDPR vastly expanded the territorial scope of application as compared to the DPD. The GDPR applies to data controllers and processors established in the EU, regardless of whether the processing takes place in the EU or not.[120] Article 3 and Recitals 22-25 of the GDPR provide that the regulation also applies to non-EU based organizations if they process the personal data of individuals in the EU obtained through offering them goods or services or through monitoring their behavior.[121] Non-EU based data controllers and processors to which the regulation applies must appoint a representative in the EU.[122] Moreover, the GDPR's extraterritorial scope extends to limitations on transfers of data outside the EU unless the jurisdiction to which the data is being transferred meets the "adequate level of protection" standards set forth in the regulation.[123]

The GDPR was expressly drafted with extraterritorial scope, meaning that compliance with the regulation might also be required outside the EU by any companies that collected data on EU data subjects, which include not only nationals and residents of the EU, but also any natural persons located in the EU, even temporarily.[124]

---

118. Regulation 2016/679 of the European Parliment 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) [hereinafter GDPR]

119. *Id.*

120. *Id.* art. 3(1).

121. *Id.* art. 3(2) & recital 22–25.

122. *Id.* art. 27(1).

123. *Id.* art. 45.

124. GDPR Recital 14 states that the GDPR applies to "natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data." *Id.* at recital 14.

In *Google Spain*, the CJEU showed a willingness to broadly interpret the place of establishment of a data controller, consistent with the GDPR even before it was enacted. In that case, the CJEU held that Spanish law applies to Google Inc.'s processing of data because Google Spain is an establishment in Spain which is "intended to promote and sell advertising space offered by [the search] engine and which orientates its activity towards the inhabitants of [Spain]."[125] This approach reflected the Court's willingness to broadly interpret the directive and provide guidance for non-EU based data controllers as to what types of activities might be deemed to be within the scope of the GDPR.

Under the GDPR, data controllers offering goods or services to individuals in the EU can be inferred by displaying prices of goods or services in EU currencies on their website, having the option for the local language on the website that is not the language of the controller's jurisdiction, or targeting people in the EU.[126] *Weltimmo* further supports the interpretation that having a website or service in an official language of an EU country could bring a data controller within the scope of the GDPR.[127] That case provided criteria for determining a data controller's intention to target individuals in a certain jurisdiction. The CJEU held that having a website in the native language of a country could bring a data controller within the jurisdiction of that country's data protection authority.[128]

The GDPR's approach to the regulation of data protection and privacy in the EU contains both territorial and extraterritorial dimensions. By focusing on "data subjects" and the free flow of data within the internal market, it contemplates applicability to all controllers and processors that process personal data on EU data subjects, regardless of where the controllers and processors are located. By linking regulation to the location of the

125. Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja Gonza´lez, ECLI:EU:C:2014:317, ¶ 100(2) (May 13, 2014).

126. GDPR, supra note 118, at recital 23; *see also Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version 2.0,* EUR. DATA PROT. BD. (Nov. 12, 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf.

127. Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, ECLI:EU:C:2015:639, ¶ 41 (Oct. 1, 2015).

128. *Id.*

individual(s) whose data is being processed rather than simply where the data itself is deemed to be located, the GDPR expands the scope of its application to include even those organizations that are processing data outside the EU. The requirement that non-EU data controllers within the scope of the GDPR must appoint a representative in the EU also creates a direct territorial link. The EU justifies the GDPR's extraterritoriality by its fundamental rights obligations.[129]

2. E-evidence Rules

The European Commission's proposed rules of access to electronic evidence in criminal law matters (E-evidence Rules) also have extraterritorial dimensions.[130] While the Rules state that they apply to service providers who provide services in the EU,[131] this does nothing to limit their application to only those companies established within the EU or to data stored in the EU. If a service provider is not established in an EU Member State, a "substantial connection" between the service provider and the EU exists if the service provider has a significant number of users or targets users in one or more Member States.[132] Thus, just as the GDPR is not limited in application to only those companies incorporated or headquartered within the EU, so too the E-evidence Rules have an extraterritorial dimension that goes beyond prior cross-border data transfer regulations. Moreover, the E-evidence Rules require companies to appoint a legal representative in the EU to whom the production orders can be directed.[133] Both the GDPR's and the E-evidence Rules' requirement for the appointment of an EU-based representative point toward an attempt to "reterritorialize" data regulations,[134] such

---

129. Symposium, *The GDPR as* Global *Data Protection Regulation?*, 114 AJIL UNBOUND 5, 5–9 (2020).

130. Régis Bismuth, *L'extraterritorialité du Cloud Act à la lumière du projet européen E-evidence*, J. DU NET (2018), https://www.journaldunet.com/solutions/expert/69507/l-extraterritorialite-du-cloud-act-a-la-lumiere-du-projet-europeen-e-evidence.shtml.

131. *Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter "E-evidence Rules"].

132. Similar to the GDPR, this can be determined if the provider is using the local language or currency on its website, application, or service. *Id.* at recital 28.

133. *Id.* art. 7.

134. Bismuth, *supra* note 130.

that even if the extraterritorial measures are deemed excessive, the presence of the representative in the EU could be another basis for asserting jurisdiction.[135]

Interestingly, the European Commission notes that with regard to the proposed E-evidence Rules, the location of where data is stored is not a determining factor, since the decision of where to store data is made by providers, rather than by states. Chapter 1 of the E-evidence Rules states: "The Regulation also moves away from data location as a determining connecting factor, as data storage normally does not result in any control by the state on whose territory data is stored. Such storage is determined in most cases by the provider alone, on the basis of business considerations."[136]

As will be discussed further in this Article, these business considerations can have effects on users, who are largely ignorant about where their data is stored or how those decisions are made. Corporations have a tremendous amount of discretion on these choices.

C. United States

In comparison with the EU, the US does not have quite as robust a data privacy framework and tends to take a sectoral approach. In terms of territoriality and cross-border transfers of, and access to, data, the two approaches are less different than they might initially appear. In relation to the regulation of cross-border transfers of data and the link to territoriality, a number of recent developments have forced US lawmakers to make efforts to clarify some of the ambiguities surrounding such transfers, especially when the data is stored on servers abroad. Since the 1980s, the US's existing framework for regulating cross-border data transfers was the Stored Communications Act (SCA).[137] Considering the innumerable changes in technology, cloud computing, and data since then, a number of questions remained unaddressed in US law, especially with regard to cross-border data transfers. In 2018 alone, a number of developments have helped

---

135. Even though the E-evidence Rules state that "the sole designation of a legal representative does not create an establishment of the service provider," it could arguably be a basis for overcoming a lack of territoriality or jurisdiction. *See* E-evidence Rules, *supra* note 131, at ch. 1.

136. *Id.*

137. *See generally* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (1986) [hereinafter SCA].

to clarify the US approach, yet ambiguities still remain. Those developments include the *Microsoft* case and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[138]

1. The *Microsoft* Case

In *United States v. Microsoft Corp.*, the US Supreme Court dealt with the issue of whether data stored in servers abroad is subject to a US warrant.[139] Government prosecutors had issued a warrant seeking information associated with a person's email account from Microsoft, some of which was stored in a data center in Ireland.[140] One of the main issues in the case was whether the location of the data is where it is stored (e.g., on servers in a data center) as contended by Microsoft or where it can be accessed as contended by the Department of Justice.[141] Microsoft argued that the data stored in Ireland was not subject to the warrant since the Fourth Amendment of the US Constitution is not generally thought to apply extraterritorially.[142] The government's position was that since the data stored in Ireland could be accessed by Microsoft in the US, it did not exceed its warrant authority by requesting this data.[143]

On the basis of the enactment of the CLOUD Act, the Supreme Court vacated the case for mootness in April 2018 and remanded it to the lower court to do the same, as the government issued a new warrant under the CLOUD Act.[144]

2. The CLOUD Act

In an effort to address the legal ambiguities surrounding cross-border data requests in light of the *Microsoft* case and to update

---

138. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V,
132 Stat. 348 (2018) (codified in scattered sections of 18 U.S.C.) [hereinafter CLOUD Act].

139. United States v. Microsoft Corp., 584 U.S. __ (2018).

140. *Id.*

141. *See, e.g.,* Transcript of Oral Argument at 8, Microsoft v. United States, 584 U.S. __ (2018) (No. 17-2), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_9pl4.pdf.

142. *See id.* at 33–34; *see also* Brief for Respondent at 30–32, 38–44, 58, United States v. Microsoft, (2018) (No. 17-2), 2018 WL 447349.

143. *See id.* at 6–7; *see also* Brief for the United States at 41–45, United States v. Microsoft, (2018) (No. 17-2), 2017 WL 6205806.

144. *See* United States v. Microsoft, No. 17-2, slip op. at 3 (2018), https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf.

the SCA,[145] the US Congress passed the CLOUD Act in March 2018, while the *Microsoft* case was pending.[146] The CLOUD Act amends the SCA and requires providers of electronic communications services and remote computing services (providers) to provide data requested by federal law enforcement via a warrant. Data should be provided upon request regardless of where the data is stored, as long as the company is subject to US jurisdiction and the data is within the company's "possession, custody, or control."[147]

The CLOUD Act also provides for the possibility of foreign countries entering into executive agreements with the US to govern the cross-border exchange of data for law enforcement purposes in the context of serious crimes.[148] It allows for reciprocal access to data and for the possibility of submitting requests directly to the technology companies rather than solely to the US government under a MLAT where the data concerns a non-US person.[149] In a situation where there is no agreement between the countries, the CLOUD Act provides technology companies the possibility to challenge the warrant under a common law comity analysis.[150]

In cases where the countries have an executive agreement in place, providers can challenge the warrant if the person is not a US citizen or national, lawful permanent resident, corporation, or other unincorporated entity (US Person) or if there are concerns that providing the data would violate the laws of a foreign government.[151] This scenario might arise, for example, if a US-based company, or a non-US based company using a US servicer or through its US subsidiary, is collecting data on a US Person located in the EU (even if temporarily) in connection with offering goods and services to that person, and the US law enforcement authorities issue a warrant for that person's data in connection with an investigation. In such a situation, if there is no existing MLAT, the data collected and stored could be subject to

145. *See* SCA.

146. Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN.L. REV. 9, 9 (2018).

147. CLOUD Act §103(a)(1).

148. Under the CLOUD Act, requests from foreign governments cannot seek information on US Persons without a MLAT. Daskal, *supra* note 146, at 14.

149. CLOUD Act § 105(a) (to be codified at 18 U.S.C.§ 2523(b)).

150. CLOUD Act § 103(c).

151. CLOUD Act § 103(b).

both the GDPR and the CLOUD Act, regardless of whether the data is stored in the US or the EU. Should there be a conflict between the provider's duty to disclose to the US law enforcement authorities, and the individual's privacy rights and the provider's duties under the GDPR, then that provider might object to the warrant on the basis of the GDPR's privacy restrictions on the transfer of data.[152] This is especially the case if the jurisdiction where the company is located has entered into an executive agreement with the US, but not an MLAT. In such a case, it is unclear whether a data transfer would fall under the exception outlined in Article 48 of the GDPR that provides for data transfers pursuant to foreign government requests under an international agreement such as an MLAT.[153]

Like the GDPR, which expanded the territorial reach of the DPD, the CLOUD Act expanded the territorial reach of the SCA. The CLOUD Act has been criticized for its extraterritorial provisions and potential extraterritorial effects. Since its explanatory memorandum states that it applies to providers subject to US jurisdiction, European companies with US subsidiaries or those that target the US market might also fall within its scope.[154]

While companies like Google, Microsoft, Amazon, and Facebook have data centers in multiple jurisdictions and have multiple options of jurisdictional choices, these choices can have distributional consequences especially since juridical efficacy can depend on whether a person is located in the same jurisdiction as where her data is stored.[155] Someone located in a different jurisdiction as her data could be subject to a longer investigation, as requests under an MLAT can take around a year to process.[156] If there is no MLAT between the jurisdictions, the process of obtaining data from another jurisdiction can be even more time consuming than the process with an MLAT. This illustrates how decisions made by technology companies on where to store data can have important consequences for the individuals whose data

152. Since these regulations are quite recent, there have not yet been any cases discussing exactly what would happen in the case of such conflict and how it might be resolved.

153. GDPR, *supra* note 118, art. 48.

154. Bismuth, *supra* note 130.

155. *Id.*

156. Daskal, *supra* note 146, at 13.

is being collected and processed, with little to no input from them or from regulatory authorities on those decisions.

IV. RETERRITORIALIZATION

With each of the different regulatory regimes concerning cross-border data flows analyzed here, we see moves towards both extraterritoriality and a reterritorialization of data in an attempt to assert jurisdiction over it and as a way to protect the interests that are prioritized by that jurisdiction. This dynamic of extraterritorial reach combined with reterritorialization is achieved through legal mechanisms, such as those regulations described herein.

China's "data localization approach" is the most explicit example of reterritorialization, reflecting its interests in controlling the flow of information within its borders for national security reasons.[157] China, which has its own national intranet and censors internet content, has a more protectionist and non-interventionist approach to data flows. Yet its data localization requirements also have extraterritorial effects. If companies located outside of China wish to collect data on persons in China, or to engage in transfers of data across Chinese borders, they must comply with the regulatory framework under the recent Cybersecurity Law and establish data centers in China.[158]

In the EU, a move toward reterritorialization is evident in several ways. Using a "fundamental rights approach" to data protection and privacy, reterritorialization occurs through the appointment of a representative in the EU for non-EU based data controllers and through the link to the location of "data subjects" in the EU. At the same time, the GDPR has an express extraterritorial scope, one that expands the geographic reach of the prior DPD substantially.

In the US, one sees a more "private-sector friendly approach" with extraterritorial dimensions. By expressly providing for mechanisms to obtain data on US Persons, even if data is stored outside the US, the CLOUD Act attempts to resolve the ambiguities regarding the reach of government warrants beyond US

157. Cai, *supra* note 87, at 65.

158. *See id.* at 74–80. This requirement under the Cybersecurity Law applies only to CIIOs, but the Draft Data Export Measures would extend them to all network operators. *Id.*

borders. Yet it also reterritorializes by linking regulations to US-based data controllers and service providers and US Persons.[159]

Figure 1. Table comparing data transfer regulations of China, EU, and the US.

	China	EU	US
Extraterritorial Dimension(s)	Applies to network operators collecting data on Chinese data subjects	Applies to data collectors and processors processing data on EU data subjects	Applies to providers subject to US jurisdiction
Re-territorialization	Data localization requirements	Link to EU data subjects; EU representative for non-EU data controllers	Point of access, custody, or control (within the US-based company or subsidiary's possession, custody or control)
Regulatory Approach	Data localization	Fundamental rights	Private sector

Source: Author

Data localization seems to be the starkest example of attempts to reterritorialize data by requiring it to be stored on servers and in data centers within national borders as an exercise of "data sovereignty" or "cyber sovereignty." Data sovereignty "refers to a spectrum of approaches adopted by different states to control data generated in or passing through national internet

159. *See supra* Section III.C. of this Article.

infrastructure" and "to subject data flows to national jurisdictions."[160] Some scholars have identified weak and strong forms of data sovereignty, with the weak variant characterized by a data governance framework that prioritizes the private sector, while the stronger forms take robust measures to safeguard national security.[161] China can be seen as taking a strong data sovereignty approach. Other countries besides China have also mandated data localization, such as Brazil and Russia, primarily based on protecting national intelligence from foreign surveillance.[162] These countries are also on the strong side of data sovereignty, which other countries, such as the United States, view as a threat to internet freedom and the free flow of information online.[163]

The risk that data localization and strong data sovereignty impose is that this will lead to fragmentation and the rise of digital borders, or what is sometimes referred to as "Internet Balkanization."[164] The concepts of sovereignty and non-interference, if taken too far, can have deeply problematic ramifications in this context.[165] In 2011, the Council of Europe warned of the potential "adverse transboundary impact on access to and use of the Internet" that can occur through exercises of national sovereignty.[166] Excessive exercises of national sovereignty can negatively impact the openness of the internet.[167] However, digital

---

160. Dana Polatin-Reuben & Joss Wright, *An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet* 1 (July 7, 2014), https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

161. *Id.*

162. *Id.*

163. *Id.*

164. Polatin-Reuben & Wright, *supra* note 160; Christopher Kuner, Fred H Cate, Christopher Millard, Dan Jerker B Svantesson & Orla Lynskey, *Internet Balkanization gathers pace: is privacy the real driver?*, 5 INT'L DATA PRIV. L. 1, 1–2 (2015).

165. Bertrand De La Chappelle & Paul Fehlinger, *From Legal Arms Race to Transnational Cooperation*, INTERNET & JURISDICTION POL'Y NETWORK (Apr. 3, 2016), https://www.internetjurisdiction.net/publications/paper/jurisdiction-on-the-internet-global-commission-on-internet-governance.

166. Committee of Ministers, *Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet* (Sept. 21, 2011), https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8.

167. *Id.*

borders are neither a technically nor economically feasible option, even for the staunchest advocates of data localization. They would entail banning the operation of many cloud service providers who contribute to trade with that country.[168] Thus, internet fragmentation and the development of digital borders are highly unlikely.[169] The challenge of trying to bring data into a territorial sphere becomes evident given the distributed quality of data and internet protocols, but countries are still attempting to assert strong data sovereignty in this area.[170]

Each of the regulatory approaches discussed here is still bound up within variations on the concept of territoriality. Their extraterritorial reach might imply efforts to set standardized norms with universal effects, especially in the case of the EU.[171] While this Article argues against a "post-territorial" conception of data governance that presumes the territorial/ extraterritorial binary, or a conception with no relation to territory at all, data is not strictly contained within the territorial borders of the state either. Moreover, states are not the only ones who exercise authority over data, even when data is located within their borders.

V. REPURPOSING TERRITORIAL SOVEREIGNTY

This Part will survey the academic literature regarding the continued viability of territoriality to serve as the foundation for the exercise of sovereignty and jurisdiction. It will then discuss examples of non-territorial conceptions of sovereignty that existed well before the rise of digital data.

A. Corporations, Code, and Elastic Sovereignty

A number of scholars have highlighted that the continuing centrality of territoriality in the realm of cyberspace and data is not the right way forward.[172] As Mireille Hildebrandt notes, legal models for cyberspace "cannot . . . be grounded in the

168. Polatin-Reuben &Wright, *supra* note 160, at 7.

169. *Id.*

170. *Id.* at 1.

171. Cedric Ryngaert, *Whither Territoriality? The European Union's Use of Territoriality to Set Norms with Universal Effects*, *in* WHAT'S WRONG WITH INTERNATIONAL LAW?: LIBER AMICORUM A.H.A. SOONS 434–48 (Cedric Ryngaert, Erik J. Molenaar, & Sarah M.H. Nouwen eds., 2015).

172. *See* Hert & Thumfart, *supra* note 17, at 13. *See also* Daskal, *supra* note 71, at 329.

monopolistic spatiality of territorial sovereignty,"[173] requiring a reconfiguration of jurisdiction.[174] Moreover, corporations have powerful roles in this domain, as they are the ones who decide where to store data, where to establish headquarters, in which jurisdictions to establish data centers, on which person(s) to collect data, and how to mediate disputes over data across borders.[175] A narrow focus on territoriality might overlook that "[t]he age of the nomos of the code is always in danger of . . . replacement of the law (nomos) by the . . . code of de facto powers, which is a priori without that close relationship to borders and territories that characterize the political or legal nomos."[176]

As Fleur Johns has noted, "data territories" are creating new configurations of associations outside of the state-centric framework of international law.[177] Moreover, these new "territories" operate outside of the confines of the public/private divide that has remained quite dominant in Western liberal legal thought.[178] The pairing and operationalizing of list and algorithm through the use of data analytics,[179] for example, can be seen as performing a variety of forms of global governance that creates new legal relations and associations that until recently

---

173. Mireille Hildebrandt, *Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace*, 63 U. TORONTO L.J. 196, 224 (2013).

174. *Id.* at 198.

175. Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 179–240 (2018).

176. Johannes Thumfart, *Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right, Just Cyber-Warfare*, *in* AT THE ORIGINS OF MODERNITY 197, 214 (José María Beneyto & Justo Corti Varela eds., 2017). Thumfart refers to the "age of digital networks" as the "the age of the 'nomos of the code . . .'" *See id.* at 198. He refers to it interchangeably with law, and distinguishes the nomos of the code from the political or legal nomos that Carl Schmitt theorized his work, THE NOMOS OF THE EARTH IN THE INTERNATIONAL LAW OF JUS PUBLICUM EUROPAEUM (G.L. Ulmen, trans., 2006). *See id.* at 206.

177. Fleur E. Johns, *Data Territories: Changing Architectures of Association in International Law*, *in* NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 2016: THE CHANGING NATURE OF TERRITORIALITY IN INTERNATIONAL LAW 107–29 (Martin Kuijer & Wouter Werner eds., 2016).

178. Duncan Kennedy, *The Stages of the Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349, 1349 (1982).

179. "Data analytics" is "a generic term descriptor for practices that frequently entail deployment of lists-plus-algorithms." *See* Fleur Johns, *Global Governance Through the Pairing of List and Algorithm*, 34 ENV'T & PLAN. D: SOC'Y & SPACE 126, 127 (2016).

have lacked a conceptual vocabulary among lawyers.[180] Moreover, as digital data assembles new juridical relations, it challenges the role of territory as the basic defining spatial epistemology in international law.[181]

Despite the attempts by various jurisdictions to reterritorialize digital data through legal mechanisms, the territorial/extraterritorial binary does not fit neatly in this context. Even when data is stored within a particular territory, it does not necessarily mean that the state has access to or control over that data,[182] as private actors exercise primary control. The idea that digital data located or stored within a physical territory gives the state sovereign power over it is an oversimplification, as "the real control and ability to actually govern the data exists but is obviously exercised by someone else,"[183] showing that "information sovereignty cannot always be implied from territorial sovereignty."[184] The picture becomes even more complex if the state depends on a private actor located in another territorial sovereign's jurisdiction to exercise sovereignty or control over information infrastructure.[185]

The focus on territoriality as a principle defining how data transfers are regulated and governed also overlooks the important role of code, markets, and private actors in the governance of data.[186] Governance of data across borders occurs through networks of private and public actors, legal mechanisms, and technologies, like computers, data servers, undersea cables, computer code, and software. The importance of code in this context also highlights the necessity of code-writers and corporate decision-makers in determining how data transfers are configured and what kinds of relations data makes. Their power, however, is not enacted in the absence of the law—the two shape one another.[187] Moreover, these exercises of governance are not solely technical decisions, as a great deal of distributive and

---

180. *Id.*

181. *See* Rajkovic, *supra* note 54.

182. POLCAK & SVANTESSON, *supra* note 75, at 172 .

183. *Id.* at 173.

184. *Id.* at 175.

185. *Id.* at 175–77.

186. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2d Revised ed. 2006).

187. Sheila Jasanoff, *Making Order: Law and Science in Action*, *in* THE HANDBOOK OF SCIENCE AND TECHNOLOGY STUDIES 761–86 (Edward J. Hackett, Olga Amsterdamska, Michael Lynch & Judy Wajcman eds., 3d ed. 2008).

political stakes are involved—such as which laws and regulations are applicable, by what means and how quickly data can be transferred across borders, and which states receive economic benefits from having technology companies operating and storing data within their borders.

Rather than theorizing sovereignty in terms of the rising or falling power of the state as the central locus of power and authority in international law, or theorizing technology in a deterministic fashion as a source of authority that competes with law or something that always precedes legal developments, one may consider the ways in which they coproduce[188] one another. This can be done by examining how law is constitutive of the elasticity of sovereignty, how that elasticity manifests in the distribution and enablement of power to a variety of actors and agents, and how the actors and agents actively reshape the law, sovereignty, and jurisdiction.

B. Was Sovereignty Ever Territorially Bounded?

The idea of territorial jurisdiction is relatively new—it developed with the technology of modern cartography to delimit legal powers within territorial bounded spaces, whereas before, legal authority tended to be premised upon relationships of status.[189] For example, in Thailand—then called Siam—political authority was exercised over specific resources, populations, and trade routes, with territorial jurisdiction only being implemented in the late nineteenth century when British and French colonial rulers insisted on sharply drawn jurisdictional boundaries and territorial borders.[190] This conception of the space of political authority was not unique to Thailand. Indeed, in Europe, until the tenth, or even as late as the fifteenth century—and certainly not until the development of modern cartograph—relationships of kinship and common interests were what held communities together.[191]

"In effect the essential thing is to gather into groups this people which is everywhere and nowhere; the essential thing is to

188. Sheila Jasanoff, *The Idiom of Co-Production*, *in* STATES OF KNOWLEDGE: THE CO-PRODUCTION OF SCIENCE AND THE SOCIAL ORDER 1–12 (Sheila Jasanoff ed., 2004).

189. Richard T. Ford, *Law's Territory (A History of Jurisdiction)*, 97 MICH. L. REV. 843, 843 (1999).

190. *Id.* at 868–70.

191. *Id.* at 872–73.

make them something we can seize hold of."[192] This quote offers one view of the control of populations as something necessary for exercising governance over them. Indeed, some of the foundational activities of the state have long been bringing populations under its control, settling them, classifying them, and taxing them.[193] One of the state's primary activities is also the act of "territorializing" and "reterritorializing"—even things which are not explicitly within its borders. What can be territorialized and brought within the jurisdiction of the state can be measured and managed, and therefore also "civilized," as James C. Scott has shown with regard to populations.[194] Interestingly, even in the context of migration, one sees disputes over what constitutes the ambit of the state's territory when migrants need rescuing at sea, illustrating how states also repurpose territoriality to avoid legal obligations, in contrast to attempts to territorialize things to manage them.

On the other hand, in the context of imperialism, from Ancient Rome to informal imperialism, the exercise of authority and asserted jurisdiction over people, activities, and territories have long existed outside the confines of territorial borders. While extraterritorial jurisdiction is not new, even today, jurisdiction is seldom exercised within strictly bounded spaces according to mapped territorial borders. What we see also in the data context is the idea that data is everywhere and nowhere in particular, and that states and regulatory authorities are attempting to reterritorialize it to justify their exercise of sovereignty and to bring data under their control based on their cultural, political, and economic interests.[195]

Indeed, the idea of "national interest" in asserting jurisdiction extraterritorially is also malleable, as can be seen in the differing results in human rights cases in the United States, such as

---

192. JAMES C. SCOTT, THE ART OF NOT BEING GOVERNED: AN ANARCHIST HISTORY OF UPLAND SOUTHEAST ASIA 98 (2010) (citing French officer, Algeria, 1845).

193. *Id.* at 98–99; *See generally* JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED (1998).

194. SCOTT, *supra* note 192, at 98–99.

195. This is consistent with analyses finding that judicial discourse surrounding assertions of jurisdiction in cases of extraterritoriality tends to be premised on language relating to membership, territory, or interests. Robert Malley, Jean Manas & Crystal Nix, *Constructing the State Extraterritorially: Jurisdictional Discourse, the National Interest, and Transnational Norms*, 103 HARV. L. REV. 1273, 1280 (1990).

Filartiga v. Pena-Irala[196] and *Tel-Oren v. Libyan Arab Republic*.[197] Exercises of jurisdiction produce and define the state rather than the other way around.[198] Rather than bounded by territorial borders or with any fixity with regard to the communities over which it claims (extraterritorial) jurisdiction, their locations, or the types of issues that reflect the state's so-called "interests", the state can be thought of as a series of jurisdictional assertions, and with each one, it creates new normative communities.[199] As Robert Malley, Jean Manas, and Crystal Nix argue "no one is entirely 'part of' the state, just as no one is totally excluded from it: no one person is subject to its sovereignty or jurisdictional power for all purposes, and all persons are subject to it for some."[200]

Moreover, as Richard T. Ford argues, territorial jurisdiction produces political subjectivity.[201] "The jurisdictional boundary does more than separate territory; it also separates types of people: native from foreign, urbanites from country folk, citizen from alien, slave from free."[202] Ford also alludes to the role of technology in helping produce political subjectivity through jurisdiction. Indeed, jurisdiction is formed by and practiced through technologies. Whether through cartographic maps, normative technologies of international legal principles, or contemporary data analytics, technology and jurisdiction are both shaping and shaped by the other. In turn, one might argue, that it is through the assertion of sovereign jurisdiction and through technology that new political communities and new forms of political subjectivity are being produced today.

CONCLUSION

The idea of a territorially-bounded sovereign has long been challenged, despite its enduring significance in international

196. Filartiga v. Pena-Irala, 630 F.2d 876 (2d Cir. 1980) (finding national interest applied to a case involving a Paraguayan police official's torture and killing of Paraguayan citizen).

197. Tel-Oren v. Libyan Arab Republic, 726 F.2d 774 (D.C. Cir. 1984) (per curiam), *cert. denied*, 470 U.S. 1003 (1985) (finding there was no national interest in asserting jurisdiction over bus attack in Israel).

198. Malley, Manas & Nix, *supra* note 195 at 1295–96.

199. *Id.* at 1304.

200. *Id.* at 1296.

201. Ford, *supra* note 189, at 844.

202. *Id.*

law. While there are many theorizations and critiques of sovereignty in political and international legal theory, few have highlighted the role of technology in shaping and giving meaning to the concept of sovereignty in its multiple manifestations. Sovereignty and jurisdiction today are practiced and effectuated in part through technologies.

The movement of digital data across borders is enabling new geographies of private and public power untethered to traditional conceptions of territoriality. Yet data regulations still attempt to create a link to territorial sovereignty and jurisdiction. While cyberspace and data flows may "escape geography"[203] in one sense, it is evident that they are also deeply intertwined with it.[204] Through a comparative analysis of data transfer regulations in three jurisdictions, namely China, the EU, and the US, it is apparent that a dual logic exists with regard to data and territoriality in each of the regulatory approaches. It also appears that there is a move away from pure territoriality towards extraterritoriality. At the same time, there is an attempt at reterritorializing data by locating data where infrastructure, data subjects, or data controllers are located. Each jurisdiction reflects a different regulatory approach, with China's data localization approach having the strongest link to territoriality. What these regulatory approaches have in common is the presumed territoriality/extraterritoriality binary with regard to data transfers and data governance, despite the challenges they pose to that presumption.

The elasticity of sovereignty has effects on who can exercise authority and power over cross-border transfers of data. While regulatory authorities are attempting to govern these transfers, which seemingly defy the boundedness of traditional conceptualizations of territorial sovereignty, they do not do so in isolation. A narrow focus on territoriality may overlook the role of corporations, code and code-writers, markets, and other data governance agents. The elasticity of sovereignty means that exercises of authority and governance over data are multiple and contingent, thus ultimately becoming functions of power. The question is, then, how to challenge those exercises of power to repoliticize social problems rather than have them managed

---

203. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD vii (2006).

204. Julie E. Cohen, *Cyberspace As / And Space*, 107 COLUM. L. REV. 210, 212–13 (2007).

within "global expert regimes,"[205] including regimes of both legal and technological expertise.

205. Koskenniemi, *supra* note 14.