Territoriality, Technology, and National Security

Zachary D. Clopton†

Across various contexts, parties and courts have pressed for territorial rules in cases implicating technology and national security. This Essay suggests that presumptively territorial approaches to these questions are misguided. Territorial rules do not track the division of authority or capacity among the branches, nor are they effective proxies for the important interests of regulators or regulatees. On issues of technology and national security, territorial rules seem particularly ill suited: territorial rules aspire to certainty, but technology makes it harder to define "territoriality" in a consistent and predictable way; technology weakens territoriality as a proxy for policy goals because data often move in ways disconnected with the interests of users and lawmakers; and technology makes it easier for public or private actors to circumvent territorial rules (often without detection), thus interfering with the existing allocation of policymaking authority. This Essay explores these themes with respect to the Stored Communications Act, electronic surveillance law, and court-access doctrines in criminal and civil litigation. The conclusion is that territorial approaches in such cases may have been wrong when first adopted or may have succumbed to desuetude in the intervening years.

INTRODUCTION

Among the most prominent legal issues arising from the global war on terror have been questions regarding the extraterritorial reach of the US Constitution. How (if at all) does the Fourth Amendment apply to global surveillance?[1] What rights are afforded to detainees held outside the United States?[2] What is the appropriate division of authority among the branches of government with respect to overseas military

† Assistant Professor of Law, Cornell Law School. I am grateful to Daniel Abebe, Anthony Colangelo, John Coyle, Paul Crane, Aziz Huq, Samuel Issacharoff, David Moore, and the participants in the *University of Chicago Law Review* Symposium for their thoughtful comments.

1 See generally, for example, Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 Stan L Rev 285 (2015).

2 See, for example, *Boumediene v Bush*, 553 US 723, 732 (2008) (asking "whether [aliens detained at Guantánamo Bay, Cuba,] have the constitutional privilege of habeas corpus").

operations?[3] Although these constitutional questions have garnered headlines, questions about the extraterritorial scope of US law also have important subconstitutional dimensions: When and how should statutes, executive orders, and judicial doctrines apply extraterritorially?

This Essay suggests that presumptively territorial approaches to these questions are misguided. Territorial rules do not track the division of authority or capacity among the branches, nor are they effective proxies for the important interests of regulators or regulatees. On issues of technology and national security, territorial rules seem particularly ill suited:

- Territorial rules aspire to certainty, but technology makes it harder to define "territoriality" in a consistent and predictable way.
- Technology weakens territoriality as a proxy for policy goals because data often move in ways that are disconnected with the interests of users and lawmakers.
- Technology makes it easier for public and private actors to circumvent territorial rules (often without detection), thus interfering with the existing allocation of policymaking authority.

Therefore, when regulating national security and technology, alternatives to territorial rules are likely appropriate.

This Essay proceeds in four parts. Part I discusses territoriality in general, explaining that territorial rules are too easily treated as presumptive. The balance of the Essay applies the lessons of Part I to three issues related to technology and national security: the Stored Communications Act[4] (SCA), electronic surveillance law, and court-access doctrine. Nothing here is meant to suggest that modern technology is unique or that national-security cases are exceptional. Instead, I argue that these technology/national-security challenges give us an opportunity to reevaluate territorial doctrines that may have been wrong when first adopted or that may have succumbed to desuetude in the intervening years.

---

[3] See, for example, *Libya and War Powers: Hearing before the Committee on Foreign Relations*, 112th Cong, 1st Sess 7, 12–14 (2011) (statement of Harold Koh, Legal Adviser, US Department of State) (discussing the Constitution and the War Powers Resolution).

[4] Electronic Communications Privacy Act of 1986 § 201 ("Stored Communications Act"), Pub L No 99-508, 100 Stat 1848, 1860–68, codified as amended at 18 USC § 2701 et seq.

I. TERRITORIALITY

Across many areas of law, courts apply territorial rules to decide questions of substance and procedure.[5] Although particular circumstances may justify territorial rules[6] and particular texts may expressly call for them,[7] a presumption as to territorial scope is unjustified on either formalist or functionalist grounds, and technology/national-security cases exacerbate these concerns.

Formalist arguments for territorial rules depend on legal distinctions among the branches that track territoriality. The Constitution, though, does not draw such distinctions in text or even in gloss—there may be different rules for *foreign affairs*,[8] but that is different from saying that there are different rules for *foreign territory*. Technology makes extraterritoriality an even worse proxy for foreign affairs, as it has become easier to affect foreign relations without physically crossing an international border. Subconstitutionally, courts have suggested that territory should serve as a presumptive measure for legislative intent because "Congress is primarily concerned with domestic conditions."[9] But as many scholars have recognized,[10] this assumption is not necessarily warranted: Congress is often concerned with

---

5 See, for example, *Equal Employment Opportunity Commission v Arabian American Oil Co*, 499 US 244, 248 (1991) (noting that "Congress legislates against the backdrop of the presumption against extraterritoriality"); *United States v Verdugo-Urquidez*, 494 US 259, 266–67 (1990) ("[I]t was never suggested that the [Fourth Amendment] was intended to restrain the actions of the Federal Government against aliens outside of the United States territory."); *Sun Oil Co v Wortman*, 486 US 717, 722 (1988) ("This Court has long and repeatedly held that the Constitution does not bar application of the forum State's statute of limitations to claims that in their substance are and must be governed by the law of a different State.").

6 Rules about real property, for example, seem like good candidates for this distinction, though even in that context one can imagine spillover effects that may justify extraterritorial property law. See, for example, Jack L. Goldsmith and Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L J 785, 795 (2001) (noting that nuisance law may apply extraterritorially).

7 For example, prior to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub L No 107-56, 115 Stat 272, the prohibition on providing material support for terrorist activities was expressly territorial. 18 USC § 2339A (2000).

8 See, for example, *American Insurance Association v Garamendi*, 539 US 396, 414–15 (2003) (explaining that the historical gloss on executive power gives the president "a degree of independent authority to act" in foreign affairs).

9 *Foley Bros, Inc v Filardo*, 336 US 281, 285 (1949). See also *Morrison v National Australia Bank Ltd*, 561 US 247, 255 (2010).

10 See, for example, Zachary D. Clopton, *Replacing the Presumption against Extraterritoriality*, 94 BU L Rev 1, 13–15 (2014).

external conditions and their consequences.[11] When regulating national security and technology, this territorialist assumption is an even worse fit with reality. And because technology may lower the costs of international movement[12] (for example, the movement of data), regulated entities may more easily evade territorial laws while effecting territorial consequences.

Functionalist explanations exist for territorial rules as well, but they too are unpersuasive. Some courts and commentators have argued that territorial rules respect foreign sovereignty,[13] but for the same reasons that Congress's concerns are not territorially bounded, foreign states' interests will not always track territorial lines.[14] Others have suggested that due process justifies territoriality because extraterritorial parties will lack notice that a statute applies to them.[15] Yet notice may track nonterritorial connections as well: were an individual to use technology to threaten US national security from abroad, the application of US law to that conduct would not be wholly unexpected.[16]

Another functionalist justification for a territorial presumption, or indeed any presumption, is the desire for certainty. Whether a rule is designed to estimate legislative preferences or to elicit them,[17] the purpose of picking a clear rule is to "preserv[e] a stable background against which Congress can legislate."[18] Clear rules also aim to create stability and predictability

---

11 Indeed, as Professor Lea Brilmayer put it: "[I]n the vast majority of cases, legislatures have no actual intent on territorial reach." Lea Brilmayer, *Interest Analysis and the Myth of Legislative Intent*, 78 Mich L Rev 392, 393 (1980) (emphasis omitted).

12 See, for example, David Hummels, *Transportation Costs and International Trade in the Second Era of Globalization*, 21 J Econ Persp 131, 151–52 (Summer 2007) (noting that technology has lowered the cost of air shipping).

13 See, for example, *Arabian American Oil*, 499 US at 248 (avoiding unintended clashes with foreign nations); *McCulloch v Sociedad Nacional de Marineros de Honduras*, 372 US 10, 20–22 (1963) (avoiding conflict with the laws of Honduras). See also Clopton, 94 BU L Rev at 8 (cited in note 10) (discussing the historical and functional roots of the presumption against extraterritoriality).

14 For example, the bases of jurisdiction in international law, which are broader than mere territory, offer some suggestion of the scope of national interests. See Restatement (Third) of Foreign Relations Law of the United States §§ 401–33 (1987).

15 See, for example, Anthony J. Colangelo, *A Unified Approach to Extraterritoriality*, 97 Va L Rev 1019, 1026–27 (2011).

16 See Clopton, 94 BU L Rev at 18–19 (cited in note 10).

17 See, for example, Einer Elhauge, *Preference-Eliciting Statutory Default Rules*, 102 Colum L Rev 2162, 2165–66 (2002) (arguing that when preferences are unclear, default rules that provoke or elicit legislative responses are often better than judicial attempts to estimate the legislature's preferences).

18 *Morrison*, 561 US at 261–63 (arguing in favor of employing a presumption against extraterritoriality).

for regulated parties as well as enforcers.[19] But it turns out that territorial rules have not lived up to their promise of reducing decision costs. Even in low-tech circumstances, the meaning of "territoriality" has vexed commentators and courts.[20] Modern technology deepens the challenge of defining what counts as "territorial." Regarding data, for example, does territoriality refer to the location of the source, the recipient, the storage, or the government access? Certainty may be important and clear rules may be desirable, but territoriality does not achieve these ends.

Technology also creates uncertainty even if the lawmaker declares a clear definition of "territoriality." For one, data may be duplicated or partitioned for the purposes of transfer and storage without the knowledge of any relevant user.[21] So even though the physical locations of data may be certain, those locations may be completely disconnected from any relevant interest of the technology's users or regulators. Technology may also allow regulated entities to cheaply evade territorial rules. Congress may be certain in its purpose of prohibiting domestic eavesdropping, but what if private entities or government officials manipulate domestic communications so that they pass briefly through foreign territory for the purpose of interception? In these ways, technology not only adds uncertainty to the meaning of "territory" but also may result in unpredictable (though perhaps intentional) changes to seemingly settled expectations.

A final but important functionalist argument for territoriality is the separation of powers.[22] There is no shortage of judicial decisions and scholarly articles suggesting that there are functional reasons to assign different responsibilities in matters of

---

19 See, for example, *Hertz Corp v Friend*, 559 US 77, 94–95 (2010) (espousing the benefits of a clear jurisdictional rule for corporations in organizing their behavior and for plaintiffs suing those businesses).

20 In *Morrison v National Australia Bank Ltd*, 561 US 247 (2010), for example, the Court explained what constituted "territoriality" under the Securities Exchange Act of 1934. Id at 261–65. The decision, though framed as intuitive, was surprising to many observers and upset decades of settled circuit precedent. See id at 274–86 (Stevens concurring); Lea Brilmayer, *The New Extraterritoriality:* Morrison v. National Australia Bank*, Legislative Supremacy, and the Presumption against Extraterritorial Application of American Law*, 40 Sw L Rev 655, 667–68 (2011) (criticizing *Morrison*'s "judicial creativity").

21 See Jennifer Daskal, *The Un-territoriality of Data*, 125 Yale L J 326, 366–68 (2015) (collecting sources).

22 See Curtis A. Bradley, *Territorial Intellectual Property Rights in an Age of Globalism*, 37 Va J Intl L 505, 550–61 (1997) (defending territoriality on separation of powers grounds).

foreign affairs.[23] For example, some argue that courts should take a backseat to the political branches in foreign relations cases[24] or that the division of labor between the executive and Congress might vary in foreign policy.[25] Even if these views are accepted, that does not mean that territorial rules should govern. As noted above, territoriality does not delineate the "delicate" foreign affairs issues that courts might avoid.[26] Nor does it track expertise or experience that might justify an alternative separation of powers framework for foreign relations.[27]

Separation of powers arguments also raise a baseline question: What is the proper balance among the branches? This is not the place to directly answer this question. What may be said, though, is that given some balance of power at time t, we should be dubious about new arrangements at time $t + 1$ that result from changing technology rather than from deliberate action among the branches. For the same reasons that territoriality does not provide certainty to regulated parties, it also does not create certain and stable divisions among the branches of government. For similar reasons, we should also be concerned when technology at time $t + 1$ allows private parties to undercut a branch's capacity to carry out its role in the interbranch scheme set at time t. In a related context, Professor Orin Kerr has advocated for a response to technology that constitutes an "equilibrium-adjustment."[28] Kerr has argued that technology alone should not expand or

---

[23] See, for example, *United States v Curtiss-Wright Export Corp*, 299 US 304, 319–22 (1936) (discussing the greater executive discretion with statutes regarding foreign affairs); Harlan Grant Cohen, *Formalism and Distrust: Foreign Affairs Law in the Roberts Court*, 83 Geo Wash L Rev 380, 386–87 (2015); Daniel Abebe and Aziz Z. Huq, *Foreign Affairs Federalism: A Revisionist Approach*, 66 Vand L Rev 723, 727–31 (2013); Derek Jinks and Neal Kumar Katyal, *Disregarding Foreign Relations Law*, 116 Yale L J 1230, 1236–38, 1248–49 (2007); Eric A. Posner and Cass R. Sunstein, Chevron*izing Foreign Relations Law*, 116 Yale L J 1170, 1202 (2007).

[24] See, for example, Posner and Sunstein, 116 Yale L J at 1204–07 (cited in note 23).

[25] See, for example, *Curtiss-Wright*, 299 US at 319–22 (discussing the president's unique role in foreign affairs).

[26] See *United States v Palmer*, 16 US (3 Wheat) 610, 634–35 (1818).

[27] See, for example, Jinks and Katyal, 116 Yale L J at 1245–49 (cited in note 23) (questioning whether the executive has the proper expertise and accountability to be due greater deference in foreign affairs).

[28] Kerr, 67 Stan L Rev at 321 (cited in note 1); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv L Rev 476, 481 (2011). Professor Lawrence Lessig's notion of constitutional "translation" provides another relevant analogy. Lawrence Lessig, *Translating Federalism:* United States v Lopez, 1995 S Ct Rev 125, 214. There are surely countless other potential analogies.

restrict government power under the Fourth Amendment.[29] Here, I suggest that technology alone should not alter the separation of those governmental powers. And because technological changes have transformed the extraterritorial capacities of the branches, territorial rules should be updated to maintain the separation of powers (at least until those questions are directly confronted).

II. TERRITORIALITY AND THE SCA

On December 4, 2013, a magistrate judge in the United States District Court for the Southern District of New York issued a warrant under the SCA authorizing the DOJ to search and seize information from Microsoft that was associated with specific e-mail accounts.[30] Under the SCA, the government may seek disclosure of stored communications in three tiers.[31] With respect to Microsoft, the Government invoked the highest tier—the SCA warrant—under which it may obtain from the Internet service provider (ISP) any opened or unopened e-mails without notice to the user.[32] The court may issue an SCA warrant "using the procedures described in the Federal Rules of Criminal Procedure" (FRCrP),[33] which require probable cause.[34]

In response to the Government's request for an SCA warrant, Microsoft filed a motion to quash the warrant as applied to information stored on Microsoft-owned servers in Ireland.[35] Microsoft argued that, because federal courts cannot issue extraterritorial warrants under FRCrP 41,[36] the SCA's warrant provision should be interpreted to apply only to data stored within the territory of the United States.[37] Microsoft also argued that the presumption

---

29 Kerr, 67 Stan L Rev at 289–90 (cited in note 1).

30 See *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*, 15 F Supp 3d 466, 467–68 (SDNY 2014) ("Microsoft").

31 See 18 USC § 2703(a)–(d). See also Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208, 1218–20 (2004).

32 See 18 USC § 2703(b)(1)(A).

33 18 USC § 2703(a).

34 See FRCrP 41(d)(1).

35 *Microsoft*, 15 F Supp 3d at 468. See also Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located outside the United States, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp*, Case No 13-2814, *1 (SDNY filed June 6, 2014).

36 See FRCrP 41(b) (limiting a magistrate judge's authority in this context to the issuance of warrants to "search for and seize a person or property located within the district").

37 See *Microsoft*, 15 F Supp 3d at 470.

against extraterritoriality suggested a territorial limit for the SCA and that such a limit depended on the location of the server on which the data were stored.[38] These arguments turned not on the location or citizenship of the user but rather on the location of the stored data.[39]

This case demonstrates how technology undercuts the supposed strengths of territorial rules.[40] Data move quickly across international borders.[41] Territory thus does not achieve certainty: it is not clear whether territoriality is measured by the location of the data, the sender, the recipient, the ISP, or the government. Nor is it clear *when* territoriality is measured: If data cross jurisdictions, do we look at the time of storage, the time of search, or some time in between? Even if the territorial rule's application were clear, the rule would not be a useful proxy for individual rights or foreign interests—the location of the data may not say anything about individuals' expectations, nor may it predict whether a foreign state will have a meaningful objection to US policy.[42] Indeed, Microsoft's decision to store these data on foreign servers depended on its desire for cost-effective storage and the users' answers to e-mail registration questions.[43] In this way, a territorial approach also seems to invite strategic behavior, as regulatees may be able to choose their regulatory regime depending on how they answer Microsoft's questions.[44]

---

[38] See id at 475–77.

[39] For its part, the Government's position also had a territorial tinge, measuring the SCA against the location of the warrant recipient (that is, Microsoft). See id at 475–76.

[40] The weak version of this claim is that there should be no presumption regarding territorial scope. A stronger version is that when interpreting a statute that lays out the executive or judicial authority in technology/national-security cases, courts might apply a presumption against a presumption against extraterritoriality—that is, courts should presume that a territorial connection is not the exclusive basis on which the statute could apply. Of course, evidence of legislative intent of extraterritorial application could overcome this presumption.

[41] See Daskal, 125 Yale L J at 366–68 (cited in note 21).

[42] A foreign state might balk at US data policy, but that objection may turn on the citizenship of the user or ISP or on the content of the communication, not only the location of the server. See, for example, Alison Smale, *Germany Limits Cooperation with U.S. over Data Gathering* (NY Times, May 7, 2015), archived at http://perma.cc/VGU5-F2W9 (noting that Germany cut back on aiding US intelligence efforts after popular outrage at reports of German intelligence services spying on German firms and individuals for the NSA). Again, the international law of jurisdiction gives some indication of other relevant interests beyond territory. See note 14.

[43] See *Microsoft*, 15 F Supp 3d at 467; Daskal, 125 Yale L J at 390 (cited in note 21) (arguing that Microsoft's position leads to the bizarre result that law enforcement's access to evidence will depend on a company's decisions about cost-effective storage locations).

[44] Daskal, 125 Yale L J at 390 (cited in note 21) ("Nefarious players could manipulate data location to their advantage.").

To generalize this point, technology reduces the cost of (opportunistically) relocating digital information compared to its analog counterpart.

Despite these arguments, Professor Jennifer Daskal's recent treatment of the *Microsoft* case argues for a territorial outcome. Though as a policy matter she would like to see reform of the SCA, for separation of powers reasons she suggests that the Second Circuit should interpret the SCA not to authorize the warrant.[45] Even on separation of powers grounds, however, *Microsoft*'s artificial territorial rule raises concerns by allowing the new information technology environment to upend existing interbranch arrangements.[46] Statutory interpretation is a search for legislative intent, and it is hard to imagine Congress expecting that the scope of executive authority would turn on the fortuity of the location where data are stored—especially when the territorial rule could encourage mischief on the part of ill-intentioned users.

Indeed, in some ways, the SCA represents a model of separated powers: the legislature authorizes the collection of certain data subject to certain procedural requirements, the executive decides which communications to pursue, and the courts evaluate the propriety of those requests and entertain objections to them.[47] This is not to suggest that the SCA should be extended indefinitely. Rather, it would not be unreasonable for a court interpreting the statute to understand its scope with an eye toward reconciling the effects of dynamic technology and the background separation of powers.

Perhaps a better separation of powers argument for a narrow reading of the SCA would be that the executive is in a strong position to request legislative updating, so courts should read the SCA to elicit congressional preferences.[48] Things might be different, therefore, if the statute authorized unconstrained executive action. But the SCA includes powers *and limits*; thus,

---

45 See id at 395–97 (noting the policy and diplomatic implications of the *Microsoft* case, and urging Congress and the executive to resolve the issue).

46 See, for example, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U Pa L Rev 373, 407–08 (2014).

47 See 18 USC §§ 2701–12.

48 This argument has the feel of the rule of lenity, under which courts require a clear statement for criminal law. See, for example, *McBoyle v United States*, 283 US 25, 27 (1931). For an example of an application of the rule of lenity outside the criminal context, see Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 Va L Rev 1513, 1514 (2014).

extending its authority extraterritorially also extends its protections. Alternatively, courts might turn their focus toward eliciting executive preferences ex ante. For example, the *Chevron* doctrine offers deference to executive interpretations, provided that the agency gives notice and provides some open and (hopefully) clarifying process.[49] Doctrines such as this will not resolve every case—indeed, the DOJ did not issue such an interpretation of the SCA—but they suggest a way forward that provides incentives for notice and public deliberation.[50] Additionally, this approach has the benefit of applying a transsubstantive framework despite a temptation to adopt exceptional approaches for national-security cases.

III. TERRITORIALITY AND SURVEILLANCE AUTHORITIES

US surveillance law is a web of authorities delineated by surveillance purpose, agent, and location.[51] These boundary lines have important consequences for the scope of government powers and for the separation of those powers. When the boundary is territorial, technological advances may blur those lines—often in ways that are hidden from the relevant parties.

A useful illustration of territorial boundaries in surveillance law can be found in the Foreign Intelligence Surveillance Act of 1978[52] (FISA) and Executive Order (EO) 12333.[53] In 1978, Congress passed FISA to govern electronic surveillance for the purposes of foreign intelligence.[54] Unlike a Title III[55] law-enforcement

---

49 See *Chevron U.S.A. Inc v Natural Resources Defense Council, Inc*, 467 US 837, 865 (1984). See also Kenneth A. Bamberger, *Normative Canons in the Review of Administrative Policymaking*, 118 Yale L J 64, 75–84 (2008) (discussing the tension between *Chevron* and normative canons of statutory interpretation).

50 For example, the DOJ proposed amendments to FRCrP 41 that would have had the practical effect of increasing the FBI's extraterritorial surveillance authority. See, for example, Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance* (Just Security, Sept 16, 2014), archived at http://perma.cc/G67G-RYK3. This note is meant not to endorse or oppose this proposal but only to suggest that the FRCrP amendment process has some advantages over less public and less deliberate alternatives. See Stephen B. Burbank and Sean Farhang, *Litigation Reform: An Institutional Approach*, 162 U Pa L Rev 1543, 1546 (2014) (discussing the rulemaking process and changes in the process over time).

51 This Part focuses on territorial boundaries, but boundaries in surveillance law exist along other dimensions as well.

52 Pub L No 95-511, 92 Stat 1783, codified as amended in various sections of Titles 18 and 50.

53 See generally Executive Order 12333, 3 CFR 200.

54 See 50 USC § 1802.

warrant, which is issued by a district court, FISA surveillance may proceed based on a court order from the special Foreign Intelligence Surveillance Court (FISC) or on a certification of the attorney general.[56] FISA sets out various substantive and procedural guidelines,[57] establishes congressional reporting requirements,[58] and requires that the executive give notice of evidence obtained or derived from FISA surveillance, thus providing additional opportunities for judicial scrutiny.[59] Although some have criticized the FISA process as too permissive,[60] it is notable that FISA is a legislative enactment that sets out various authorities for and limits on executive actions that are reviewable by courts.

FISA is often described as the exclusive authorization of electronic surveillance for the purposes of foreign intelligence,[61] but it turns out that the term "electronic surveillance" does important work in that claim. "Electronic surveillance" is defined to include the acquisition of communications in the United States or as a result of the intentional targeting of a US person.[62] But these conditions do not describe all of the activities that one might think of as electronic surveillance. "[I]f an intelligence agency can construct plausible presumptions that surveillance does not 'intentionally target' a US person and when the surveillance is conducted abroad, the permissive legal regime under EO 12333 applies."[63] Unlike FISA, EO 12333 allows

---

55 Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub L No 90-351, 82 Stat 211, codified as amended in various sections of Titles 18 and 47.

56 Compare 18 USC § 2516(1) (requiring an application to "a Federal judge of competent jurisdiction" in order to intercept electronic communications), with 50 USC § 1802(a)(1) (allowing the president, through the attorney general, to "authorize electronic surveillance without a court order"), and 50 USC § 1804 (describing applications for FISC orders).

57 See 50 USC §§ 1801–11.

58 See 50 USC §§ 1807–08.

59 See 50 USC § 1806.

60 See, for example, Owen Fiss, *Even in a Time of Terror*, 31 Yale L & Pol Rev 1, 16 (2012) (noting that the use of FISA procedures in foreign intelligence gathering has undermined the traditional probable cause requirements of *Katz v United States*, 389 US 347 (1967), and *United States v United States District Court for the Eastern District of Michigan*, 407 US 297 (1972)).

61 See 50 USC § 1812(a) (noting that, with limited exceptions, FISA "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted").

62 50 USC § 1801(f).

63 Axel Arnbak and Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 Mich Telecomm & Tech L Rev 317, 321 (2015). See also *The National Security Agency: Missions, Authorities, Oversight and Partnerships* *2–3 (NSA, Aug 9, 2013), archived at http://perma.cc/UGS5-2KFQ.

some surveillance with approval from only the attorney general or the NSA director.[64] Procedural protections, including protections for US citizens, seem to be weaker under EO 12333 than FISA.[65] EO 12333 is harder to challenge in court (and perhaps in the press) because it lacks FISA's notice requirement.[66] No statute requires congressional reporting of EO 12333 activity.[67] And because it is an executive order, Congress is not a necessary party to EO 12333 updates.[68]

Across a range of surveillance authorities including FISA and EO 12333, protections and oversight are greater within the United States than abroad.[69] This may sound unremarkable, and this may indeed be a reasonable way to balance liberty and security. What is notable, however, is the way that advances in technology have changed the balance of power within this regime. Researcher Axel Arnbak and Professor Sharon Goldberg, among others, have explained how seemingly domestic Internet traffic may be captured abroad, and is thus subject to EO 12333, when lawmakers may have presumed that it would be subject to FISA.[70] The revealed MUSCULAR program, for example, invoked EO 12333 authority to intercept Google and Yahoo traffic from outside the United States.[71] Perhaps deserving of greater attention, Arnbak and Goldberg have also demonstrated the technological tools available to *intentionally divert* US Internet

---

64 3 CFR 211–13.

65 See 3 CFR 215–16. See also John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans* (Wash Post, July 18, 2014), archived at http://perma.cc/N4PU-AXFS (noting the low protections for the privacy of US citizens' communications under EO 12333).

66 See Patrick C. Toomey, *Executive Order 12333, Notice, and the Due Process Rights of Criminal Defendants* (Just Security, Aug 14, 2014), archived at http://perma.cc/F9K5-EYRP.

67 See, for example, Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued* (McClatchyDC, Nov 21, 2013), archived at http://perma.cc/8G57-N5BR (quoting then–Chair of the Senate Intelligence Committee Dianne Feinstein as arguing that Congress does not sufficiently oversee EO 12333 programs).

68 Indeed, some have claimed that the executive has inherent authority to conduct certain surveillance operations. See, for example, John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 Geo Mason L Rev 565, 589 (2007).

69 See Daskal, 125 Yale L J at 353 (cited in note 21) (arguing that "the entire statutory scheme governing foreign intelligence surveillance is premised on an assumption that persons located in the United States are entitled to greater privacy protections than those outside U.S. borders").

70 Arnbak and Goldberg, 21 Mich Telecomm & Tech L Rev at 343 (cited in note 63) (explaining that "traffic between two US endpoints that is naturally routed abroad can [ ] be collected abroad under the permissive EO 12333 regime").

71 See Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say* (Wash Post, Oct 30, 2013), archived at http://perma.cc/L4PT-KD7W.

traffic abroad.[72] There are reasons to think that the US government has the capacity to divert traffic outside the United States by using "impersonated" Border Gateway Protocol messages,[73] by subverting the domain name system mapping for a domain,[74] or by employing other network exploits.[75] And the government may argue that these newly extraterritorial data are subject to EO 12333 rather than FISA.[76]

In the terms of this Essay, these techniques highlight the weaknesses of the case for territorial rules. If the executive were to employ these tools, users and providers of information technology would be unaware of the territorial locations of their data, and the interests of policymakers at home and abroad would further diverge from territorial location. Technology also alters the interbranch dynamic in these cases: executive officials can conduct more surveillance without judicial scrutiny, congressional participation, or even internal checks at the highest levels. The lack of direct oversight has knock-on effects, because it may be more difficult for the other branches to rebalance the scales contemporaneously or in hindsight—if Congress, the courts, and the public are unaware of much of the EO 12333 surveillance, then how can they rein in the excesses that may result from myopically territorial rules?

Each branch has opportunities to scrutinize surveillance regimes. For example, Congress must reauthorize many relevant

---

72 Arnbak and Goldberg, 21 Mich Telecomm & Tech L Rev at 347–56 (cited in note 63). Technology, of course, is not a necessary ingredient to the executive's intentional manipulation of territorial rules. In the context of national-security policy, the recently released "torture report" confirmed that the executive branch strategically moved detainees to avoid judicial review predicated on territorial connections. See *Report of the Senate Select Committee on Intelligence: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program Together with Foreword by Chairman Feinstein and Additional and Minority Views*, S Rep No 113-288, 113th Cong, 2d Sess 140–41 (2014). See also Steve Vladeck, *The SSCI Torture Report,* Rasul*, and Transfers to Avoid Jurisdiction* (Just Security, Dec 9, 2014), archived at http://perma.cc/HK9U-2DNX.

73 Arnbak and Goldberg, 21 Mich Telecomm & Tech L Rev at 347–51 (cited in note 63). See also Andrea Peterson, *Researchers Say U.S. Internet Traffic Was Re-routed through Belarus. That's a Problem.* (Wash Post, Nov 20, 2013), archived at http://perma.cc/8PDU-VWNA (noting a recent rerouting of Internet traffic and explaining that rerouting presents the "opportunity for bad actors to snoop on traffic").

74 This technique may be employed extraterritorially. See Arnbak and Goldberg, 21 Mich Telecomm & Tech L Rev at 351–52 (cited in note 63).

75 See id at 355–56. See also Darlene Storm, *17 Exploits the NSA Uses to Hack PCs, Routers and Servers for Surveillance* (Computerworld, Jan 3, 2014), archived at http://perma.cc/9JCB-FNFS.

76 See Arnbak and Goldberg, 21 Mich Telecomm & Tech L Rev at 323 (cited in note 63) (drawing an analogy to the legal case for the MUSCULAR program).

provisions,[77] the Privacy and Civil Liberties Oversight Board has declared its intention to review EO 12333,[78] and judicial supervision of government surveillance is also possible.[79] And, for the reasons given here, this scrutiny should extend to the territorial rules that mark the boundaries of those regimes.

IV. TERRITORIALITY AND COURT ACCESS

An attentive reader might think that the Constitution has something to say about the overreach just described. In decisions such as *Reid v Covert*[80] and *Boumediene v Bush*,[81] the Supreme Court has acknowledged that some constitutional rights apply extraterritorially in certain circumstances.[82] So, if the government has the authority to act extraterritorially—an authority more easily exercised with modern technology—and if a governmental act potentially violates substantive rights that are extraterritorial in scope, then one might think that individuals should be able to vindicate those rights regardless of their locations. And yet, courts have layered additional, territorial limits on existing rules for court access to make those claims in criminal and civil cases.

One area in which territory may curtail court access is criminal procedure. In *United States v Hijazi*,[83] a Lebanese citizen living in Kuwait was indicted for fraud arising out of dealings with the US military in the Middle East.[84] Apart from a brief visit

---

77 See PATRIOT Sunsets Extension Act of 2011, Pub L No 112-14, 125 Stat 216, codified as amended at 50 USC §§ 1801, 1805, 1861–62.

78 See *PCLOB Announces Its Short-Term Agenda* (Privacy and Civil Liberties Oversight Board, Sept 3, 2014), archived at http://perma.cc/AWH9-TZ7S.

79 See, for example, *American Civil Liberties Union v Clapper*, 785 F3d 787, 810 (2d Cir 2015) (holding that the appellants were not precluded from suing the Government for surveillance programs carried out under the aegis of FISA).

80 354 US 1 (1957).

81 553 US 723 (2008).

82 See, for example, id at 732 (holding that aliens detained at Guantánamo "do have the habeas corpus privilege"); *United States v Verdugo-Urquidez*, 494 US 259, 277–78 (1990) (Kennedy concurring) (arguing that, while the Fourth Amendment was not violated in this case, the Constitution may apply extraterritorially when the result would not be "impracticable and anomalous"); *Covert*, 354 US at 74–75 (Harlan concurring) (arguing that the Constitution should apply extraterritorially when not "impracticable and anomalous").

83 2008 WL 4151337 (CD Ill).

84 See *In re Hijazi*, 589 F3d 401, 404–05 (7th Cir 2009) (discussing the lower court's proceedings). Hijazi's constitutional claims relied on the Due Process Clause of the Fifth Amendment and the speedy trial right of the Sixth Amendment (because his indictment sat for five years without further process). See id at 403.

years prior, which all parties agreed was unrelated to the case, Hijazi had never been to the United States, nor had he planned to come.[85] Hijazi filed a motion to dismiss, arguing that his extraterritorial prosecution violated his rights under the Constitution and exceeded the terms of the relevant statute.[86] The Government argued that unless and until Hijazi came to the United States *in person*, he should not be permitted to have a hearing on his claims.[87]

Drawing an analogy to the fugitive-disentitlement doctrine, the district court refused to address the motion to dismiss, noting that Hijazi sought "the benefit of a ruling from [the court] without the risk that, if the ruling [was] not in his favor, he appear and be arraigned."[88] Note that the court did not rule that the Constitution was territorial in scope but instead refused to entertain the motion because the defendant himself was outside US territory. The Seventh Circuit overruled this decision and ordered the district court to rule on the motion,[89] but in a recent prosecution arising from the alleged manipulation of LIBOR, the DOJ again argued that the court should reject an extraterritorial defendant's motion to dismiss an indictment: "The Court should not devote its resources to resolving claims asserted by a defendant who will not submit to its authority."[90]

It is true that an extraterritorial defendant is differently situated from a territorial one—if the motion to dismiss is denied, the extraterritorial defendant remains free. But extraterritorial indictees are still burdened,[91] and in any event, judicial abstention in these situations has the effect of accreting power

---

85 Id at 412. The Government alleged various connections to the United States, none of which involved territorial presence. Of note, the Government suggested that Hijazi's fraud was connected to the United States because "Hijazi (located in Kuwait) sent [emails] to Mazon (located in Greece) using email addresses that the government characterize[d] as 'based in the United States' (*e.g.*, Jeff.Mazon@Halliburton.com)." Id at 411.

86 Id at 405.

87 See Government's Motion to Stay Ruling on Defendant Hijazi's Second Motion to Dismiss the Indictment and to Hold Motion in Abeyance pending Arraignment, *United States v Hijazi*, Criminal Action No 05-40024, *2 (CD Ill filed Jan 24, 2008) (available on Westlaw at 2008 WL 8838781).

88 *Hijazi*, 2008 WL 4151337 at *2.

89 *In re Hijazi*, 589 F3d at 414.

90 Opposition to Defendant Roger Darin's Motion to Dismiss the Criminal Complaint, *United States v Hayes*, Case No 12-3229, *39 (SDNY filed Nov 18, 2014). The magistrate judge rejected the Government's argument and heard the motion but denied it on the merits. *United States v Hayes*, 99 F Supp 3d 409, 426 (SDNY 2015).

91 See, for example, *In re Hijazi*, 589 F3d at 407 ("As long as the indictment hangs over Hijazi, he is prejudiced even if he does not travel to the United States.").

to the executive. In the words of the Supreme Court, "the claims of individuals—not of Government departments—have been the principal source of judicial decisions concerning separation of powers and checks and balances."[92] But by conditioning individuals' court access on territorial presence, courts may ignore meaningful individual claims. This result is particularly apparent when information technology facilitates the extension of the government's investigative and prosecutorial authority. For example, imagine that the US government offers an indictment based solely on evidence gathered pursuant to the type of extraterritorial surveillance described in Part III. In cases like this one, maintaining a territorial rule in light of the executive's increased capacity produces a new (different) separation of powers outside the United States, even with respect to those constitutional provisions that purportedly apply extraterritorially.[93]

A similar story can be told with respect to the government's territorialist objections to civil litigation that seeks monetary relief. Although courts have shown some willingness to extend some constitutional rights and associated equitable remedies to extraterritorial cases, claims brought pursuant to *Bivens v Six Unknown Named Agents of Federal Bureau of Narcotics*[94] have been a different story. At least five courts of appeals have dismissed *Bivens* claims because special factors counsel against extraterritorial *Bivens* actions related to national security,[95] even in suits filed by US citizens.[96] Professor Andrew Kent, among others, has defended this territorialist practice on separation of powers grounds.[97] Meanwhile, in the takings context, courts have dismissed extraterritorial takings actions on the basis of prudential standing—again, without reference to the territorial scope of the

---

92 *Bond v United States*, 131 S Ct 2355, 2365 (2011).

93 An equilibrium adjustment might provide that if something other than territorial presence brings someone within the scope of a statute—for example, Internet contacts—then, at a minimum, that connection alone should be sufficient to challenge the statute's constitutionality in court. One might be able to make a similar proposal to expand the substantial voluntary connections required for constitutional rights to attach under *Verdugo-Urquidez*, though that issue is beyond the scope of this Essay.

94 403 US 388 (1971).

95 See Andrew Kent, *Are Damages Different?:* Bivens *and National Security*, 87 S Cal L Rev 1123, 1125–26 (2014) (collecting cases). In the words of one judge: "[T]here is a fundamental difference between courts evaluating the legitimacy of actions taken by federal officials in the domestic arena and evaluating the same conduct when taken in the international realm." *Arar v Ashcroft*, 414 F Supp 2d 250, 282 (EDNY 2006).

96 See, for example, *Vance v Rumsfeld*, 701 F3d 193, 195, 203 (7th Cir 2012) (en banc); *Lebron v Rumsfeld*, 670 F3d 540, 556 (4th Cir 2012).

97 Kent, 87 S Cal L Rev at 1192–93 (cited in note 95).

substantive right.[98] In *Atamirzayeva v United States*,[99] the plaintiff alleged that American authorities conspired to demolish her cafeteria near the US embassy in Uzbekistan and replace it with a security checkpoint.[100] The Court of Federal Claims dismissed the case because the extraterritorial plaintiff lacked prudential standing, while it explicitly acknowledged that, on the merits, "the Takings Clause of the Fifth Amendment has extraterritorial application."[101]

Bivens suits and takings claims compensate individuals for constitutional deprivations but also have consequences for executive decisionmaking. "[T]he purpose of *Bivens* is to deter the officer."[102] "[T]he Takings Clause is meant to curb inefficient takings."[103] These goals are frustrated when courts cut off meritorious suits on territorial theories. And, for reasons articulated above, there is not a solid justification for applying a territorially based rule—particularly when technology lowers the barriers to extraterritorial government conduct, which might violate the Constitution.[104] Instead, if courts endeavor to prevent technology from tipping the interbranch balance of power, court-access doctrines need to adjust to the modern national-security environment.

Nothing here should be read to say that every constitutional provision should apply in every extraterritorial case. Debates about the extraterritorial reach of the Constitution are ongoing.[105]

---

98 See Jeffrey Kahn, *Zoya's Standing Problem, or, When Should the Constitution Follow the Flag?*, 108 Mich L Rev 673, 674–76, 685 (2010) (collecting cases).

99 77 Fed Cl 378 (2007).

100 Id at 379.

101 Id at 385, 387. Courts have taken similar steps in other court-access cases as well. See Kahn, 108 Mich L Rev at 685 (cited in note 98).

102 *Federal Deposit Insurance Corporation v Meyer*, 510 US 471, 485 (1994) (emphasis omitted).

103 *District Intown Properties LP v District of Columbia*, 198 F3d 874, 887 (DC Cir 1999).

104 Imagine, for example, an extraterritorial plaintiff (US citizen or not) claiming that the US government violated her right to due process or took her property without just compensation by using a computer virus or other network attack. See, for example, Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer* (Wired, Aug 5, 2014), archived at http://perma.cc/LTC2-CCT2 (discussing the use of network investigative techniques, sometimes extraterritorially, with the goal of "giv[ing] the government access to your files, location, web history[,] and webcam for a month at a time"). See also David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks against Iran* (NY Times, June 1, 2012), archived at http://perma.cc/U36M-A5K9 (discussing the Stuxnet offensive cyberattack).

105 See generally, for example, Kal Raustiala, *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law* (Oxford 2009).

But the judiciary should not sit out those debates because of territorial court-access doctrines. And if those rights are extended extraterritorially, the judiciary should not abstain from giving them effect on territorialist grounds alone.

CONCLUSION

Modern technology butts up against the separation of powers along many dimensions discussed in this Symposium. Here, I have taken up one such dimension: the way that technology makes already-weak territorial rules appear even weaker. Whether they are used to interpret statutes, define executive power, or allocate court access, these territorial rules do not live up to their status as presumptive defaults. In some cases, the benefits of rules (as opposed to standards) will be significant, but that does not mean that territory has to be the lodestar of the chosen rule. In other cases, modern technology may have diluted the benefits of rules such that standards are more appropriate. The point here is not to determine the best solution for every case but merely to suggest that territorial rules seem to be an increasingly poor match for the modern environment.

Looking ahead, just as separation of powers concerns motivate much of the criticism of territorial rules in these cases, they also suggest potential responses. For one thing, technology/national-security cases pose hard questions for any one branch, so arrangements that encourage interbranch coordination should be valued. The interlocking participation in stored-communications access, like Professor Aziz Huq's original vision of the Fourth Amendment,[106] is not to be trivialized. Similarly, doctrines that respect congressional delegations and executive, ex ante decision-making, subject to judicial review, should be encouraged.[107] On the other hand, approaches like the territorial court-access doctrines that have the effect of knocking out one or more branches' participation should be viewed with a gimlet eye. This is especially true, of course, when the normative justifications for such rules are so weak. Finally, although I am generally skeptical of foreign affairs or national-security exceptionalism, there may be a stronger case for technology exceptionalism. In the rules/standards frame, it may be that new technologies demand

---

[106] See generally Aziz Z. Huq, *How the Fourth Amendment and the Separation of Powers Rise (and Fall) Together*, 83 U Chi L Rev 139 (2016).

[107] See notes 24, 49, and accompanying text (discussing *Chevron U.S.A. Inc v Natural Resources Defense Council, Inc*, 467 US 837 (1984)).

standards that coalesce into rules only with time. Or in the separation of powers frame, it may be that functionalist arguments for particular branch roles have force when dealing with new technologies until formal divisions can be laid out with clarity. Either way, the path forward relies on institutional responses to improve on the rigid territorial rules that tempt parties and courts.