THE UN-TERRITORIALITY OF DATA

by Jennifer Daskal*

Forthcoming, to be published by the Yale Law Journal (2015/16)

Abstract

Territoriality looms large in our jurisprudence, particularly as it relates to the government's authority to search and seize. Fourth Amendment rights turn on whether the search or seizure takes place territorially or extraterritorially; the government's surveillance authorities depend on whether the target is located within the United States or without; and courts' warrant jurisdiction extends, with limited exceptions, only to the border's edge. Yet the rise of electronic data challenges territoriality at its core. Territoriality, after all, depends on the ability to define the applicable "here" and "there," and it presumes that the "here" and "there" have normative significance. The ease and speed with which data travels across borders, the seemingly arbitrary paths it takes, and the physical disconnect between where data is stored and where it is accessed, critically test these foundational premises. Why should either privacy rights or government access to sought-after evidence depend on where a document is stored at any given moment? Conversely, why should State A be permitted to unilaterally access data located in State B, simply because technology allows it to do so, without regard to State B's rules governing law enforcement access to data held within its borders?

This article tackles these challenges. It explores the unique features of data, and highlights the ways in which data undermines long-standing assumptions about the link between data location and the rights and obligations that ought to apply. Specifically, it argues that a territorial-based Fourth Amendment fails to adequately protect "the people" it is intended to cover. On the flip side, the article warns against the kind of unilateral, extraterritorial law enforcement that electronic data encourages—in which nations compel the production of data located anywhere around the globe, without regard to the sovereign interests of other nation-states.

TABLE OF CONTENTS

* Assistant Professor, American University Washington College of Law. For helpful conversations, comments, and support, special thanks go to Bobby Chesney, Ashley Deeks, Dean Claudio Grossman, David Gray, Ryan Goodman, Amanda Frost, Ahmed Ghappour, Chimene Keitner, Orin Kerr, Amanda Leiter, Jennifer Mueller, Paul Ohm, Samuel Rascoff, Peter Swire, Carol Steiker, Stephen Vladeck, Benjamin Wittes, Lindsay Wiley; participants at New York University's Hauser Colloquium, Oct. 29, 2014; participants at the University of Texas faculty workshop, Nov. 20, 2014; participants at the Privacy Law Scholars Conference in Berkeley, CA, June 5-6, 2015 (where it was the recipient of the PLSC Young Scholars Award); two excellent research assistants, Tiffany Sommadossi and Justin Watkins; and the terrific editors at the Yale Law Journal.

INTRODUCTION

In December 2013, U.S. federal law enforcement agents served a search warrant on Microsoft, demanding information associated with a Microsoft user's web-based email account. Because the sought-after emails were located in a data-storage center in Dublin, Ireland, Microsoft refused to turn them over, claiming that the government's warrant authority does not extend extraterritorially, and thus the warrant was invalid. The government, along with the magistrate judge and district court, disagreed—concluding that the relevant reference point was the location of Microsoft, not the location of the data.[1] Because the data could be accessed and

[1] *See* Brief for Appellee, *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft, no. 14-2985-CV (2d Cir. Mar. 9, 2014) [hereinafter Appellee Brief, Microsoft] (construing an ECPA warrant as a form of compelled disclosure, akin to a subpoena, under which the location of the provider controls); Transcript, Oral Argument, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 2014 U.S. Dist. LEXIS 133901, at *1 (S.D.N.Y, July 31, 2014) (13-MJ-2814) [hereinafter Oral Argument Tr.]; *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. Apr. 25, 2014).

controlled from Microsoft employees within the United States, this was a territorial, not extraterritorial, warrant. It was therefore valid.[2]

The question of where the relevant state action takes place when the government compels the production of emails from an Internet Service Provider (ISP) is one of first impression, now being litigated before the Second Circuit. It has garnered the attention of communication companies throughout the United States, the Irish government and European Parliament, media outlets, the U.S. Chamber of Commerce, and a wide array of commentators.[3] In a strongly worded letter, the former European Union Justice Commissioner warned that execution of the warrant may constitute a breach of international law—a sentiment echoed in many of the amicus briefs filed in support of Microsoft.[4] But such a statement simply assumes the answer to the key question that the case poses: Where does the key state action occur? At the place where data is accessed? Or the place where it is stored? If the relevant state action occurs within the United States, as the U.S. government claims, there was no breach of Ireland's sovereignty, and no violation of international law.

The dispute has laid bare the extent to which modern technology challenges basic assumptions about what is "here" and what is "there." In so doing, it highlights the centrality of territoriality to our understanding of the relevant statutory and constitutional provisions governing searches and seizures of digitized information and challenges its dominance. After all, territorial-based rules of the game are premised on two key assumptions: that objects have an observable, identifiable, and stable location, either within the territory or without; and that the location matters—that it is and should be determinative of the statutory and constitutional rules that apply. Data challenges both of these premises. First, the ease, speed, and unpredictable ways in which it flows across borders make location of data

---

[2] *See* Appellee Brief, Microsoft, at 32-33 (rejecting claim that there is anything extraterritorial about Microsoft being compelled to disclose to U.S.-based law enforcement officials records under its control); Oral Argument Tr.*, supra,* note 1, at 69; *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*,* 15 F. Supp. 3d at 476 (concluding that warrant "places obligations only on the service provider to act within the United States.").

[3] Amici on behalf of Microsoft in the Second Circuit include a list of who's who from the telecommunications industry, including Apple, Amazon.com, Accenture PLC, AT&T, Verizon, Cisco, Hewlett-Packer, Ebay, Inc; the U.S. Chamber of Commerce and the National Association of Manufacturers; companies representing a range of media outlets, including ABC, Fox News, Forbes, The Guardian, McClatchy, NPR, and the Washington Post; the Irish government; the vice-chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; computer and data science experts writing to clarify how the cloud operates; and non-profits. Links to the amici briefs are available here: http://digitalconstitution.com/about-the-case/. *See also* Editorial, *Adapting Old Laws to New Technologies,* N.Y. TIMES, July 27, 2014, at A16; Orin Kerr, *What Email Protections Apply to E-mail Stored Outside the United States*, WASH. POST, July 7, 2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/. Communication companies warn of a devastating loss of business if the government prevails.

[4] Viviane Reding, Letter to Sophie in't Veld, 24 June 2014 (on file with author).

an unstable and often arbitrary determinant of the rules that apply. Second, the physical disconnect between the location of data and the location of its user, with the user often having no idea where his or her data is stored at any given moment, undercuts the normative significance of data location.

This is not to say that tangible objects are immovable, or that they are always co-located with their owner. Both people and objects travel from place to place. And people can, and often are, separated from their tangible property by an international boundary. But the movement of people and their physical property is a physically observable event, subject to readily apparent technological and physical limitations affecting how quickly bodies and tangible things can travel through space. By contrast, the movement of data from place to place often happens in a seemingly arbitrary way, generally without the conscious choice—or even knowledge—of the data "user" (by which I mean the person with a reasonable expectation of privacy in the data, such as the user associated a particular email account).[5] An email sent from Germany, for example, may transit multiple nations, including the United States, before appearing on the recipient's device in neighboring France. Contact books created and managed in New York may be stored in data centers in the Netherlands. A document saved to the cloud and accessed from Washington, D.C., may be temporarily stored in a data storage center in Ireland, and possibly even copied and held in multiple places at once. These unique features of data raise important questions about which "here" and "there" matter, and thus call into question the normative significance of long-standing distinctions between what is territorial and what is extraterritorial. Put bluntly, data is destabilizing territoriality doctrine.

Data also challenges territoriality's twentieth-century companion criteria, citizenship and national ties, as determinative of the constitutional and statutory rules that apply. It is now widely accepted that both citizens and non-citizens with substantial voluntary connections to the United States enjoy basic constitutional protections, including the protections of the Fourth Amendment, even when they are located outside the United States' borders.[6] Conversely, the Fourth Amendment does not protect non-citizens outside the United States, absent sufficient voluntary connections to the nation.[7] Thus, territoriality doctrine, at least for constitutional purposes, involves a two-part inquiry into territoriality and target identity—with identity turning on the depth of the target's connections to the United States.

---

[5] The question as to who counts as having a reasonable expectation of privacy in the data is itself a contested issue worthy of its own extended analysis. *See* discussion *infra* Part II(E).

[6] *See, e.g.*, Reid v. Covert, 354 U.S. 1 (1957) (extending jury trial rights to citizen-dependents of the military located abroad); David J. Barron, Acting, Assistant Attorney General, Office of Legal Counsel, Memorandum to the Attorney General, Re: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations Against Shaykh Anwar al-Aulaqi, July 16, 2010 at 38 [hereinafter OLC al-Aulaqi Memo] ("Because al-Aulaqi is a U.S. citizen, the Fifth Amendment's Due Process Clause, as well as the Fourth Amendment, likely protects him in some respects even while he is abroad.")

[7] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

But just as data highlights the arbitrariness of making the location of mobile 0s and 1s determinative of the rights and obligations that apply, data challenges the companion focus on identity. One's digital footprints are neither observable nor readily identified as "belonging" to a particular person. While an Internet Protocol (IP) address might reveal a user's location, the use of anonymizing services and other tools designed to protect one's privacy (or evade detection) can make even the task of identifying a data user's location exceedingly difficult, let alone the user's citizenship or depth of connections with the United States.[8] While similar identification problems occur in the world of tangible property, the ubiquitous and intermingled nature of data compound the problem of identification in degree and kind. This problem is particularly acute in the context of mass surveillance, where the sheer quantity of data collected necessitate the use of presumptions as a basis for establishing identity. The vast quantity of data collected means that even a low error rate will yield large quantities of data associated with misidentified users.

This article takes up the challenge that data—in particular its mobility, interconnectedness, and divisibility—poses to territoriality doctrine, and its associated focus on user identity. To be clear from the outset, I do not purport to provide all of the answers, a task that requires far more than a single article. Rather, the aim of this article is to expose the fiction of territoriality in a world of highly mobile, intermingled, and divisible data, to highlight flaws in the doctrine, and to suggest alternative approaches to thinking about the scope of the Fourth Amendment, rules governing the acquisition of foreign intelligence information, and the territorial limits on law enforcement jurisdiction.

The article proceeds in three parts. Part I begins by analyzing long-standing presumptions against the extraterritorial of the law, examining its dominant, and often confused, constitutional, statutory, and jurisdictional applications. The section elucidates the ways in which territorial-based Fourth Amendment and territorial-based distinctions embedded in the statutory scheme governing acquisition of foreign intelligence information operate as a proxy for the now-dominant view that only certain "people"—namely U.S. citizens, non-citizens with substantial voluntary connections to the United States, and those physically present in the United States—are entitled to core privacy rights vis-à-vis the U.S. government.

By comparison, territoriality in the context of warrant jurisdiction, while equally entrenched, serves a very different function. Whereas the

[8] *See, e.g.*, See Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division, Department of Justice, to Reena Raggi, Chair, Advisory Committee on the Criminal Rules, Sep. 18, 2013 [hereinafter Raman Letter] at 2, available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf (describing the increased use of sophisticated anonymization technologies); Craig Timberg & Ellen Nakashima, *FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance*, Wash. Post (Dec. 16, 2013), http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (describing the difficulty of determining the identity and location of a known Internet user).

Fourth Amendment imposes *restrictions* on the government's otherwise unfettered search and seizure authority, warrants provide the government the affirmative *authorization* to search and seize. Territorial-based limits on warrant jurisdiction are grounded in respect for other nations' sovereignty and the long-standing international law prohibition on the unilateral exercise of law enforcement in another state's territory, coupled with an understanding of the practical difficulties and the policy consequences of doing so.

Part II highlights the ways in which data challenges key presumptions at the core of territoriality doctrine across each of these areas of the law. This section identifies central differences between data and its tangible counterparts, focusing in particular on its mobility, divisibility, and interconnectedness, as well as the location independence of data and its user—referring to the user's lack of knowledge or explicit choice as to the location of his or her data at any given moment.

Finally, in Part III, I argue that these differences between data and its tangible counterparts matter, but in the exact opposite way than the government has suggested. They both compel a rejection of a territorial Fourth amendment and highlight the dangers of the kind of unilateral, extraterritorial law enforcement that data permits, and perhaps encourages. More specifically, I argue that the intermingling and mobility of data means that territorial distinctions at the heart of the Fourth Amendment and the statutory scheme governing foreign intelligence surveillance no longer serve the interests they are designed to protect, at least as applied to the acquisition (seizure) of data. Large quantities of protected person data are being "incidentally" seized under the much more permissive rules governing the collection of non-protected person information. This reality calls for a rethinking of the Fourth Amendment's reach.

Specifically, I argue that the Fourth Amendment should presumptively apply to the search and seizure of data, regardless of where the data or target is located, and regardless of the nationality and identity of the target. The presumption could be overcome if and only if the government can conclusively determine that *none* of the parties to the communication or with an ownership interest in the data are U.S. persons with Fourth Amendment rights. As should be clear, such a proposal is neither inherently rights-protective nor rights-restrictive; it simply applies a presumption in the uniform application of whatever rules are adopted, absent a conclusive determination that the search or seizure does not implicate any U.S. persons Fourth Amendment interests.

Turning to warrant jurisdiction, the arbitrariness and fluidity of data location expose the problems with territorially-limited warrants. This does not mean, however, that these territorial limits ought to be unilaterally rejected without consideration of the countervailing policy considerations. The kind of unilateral, extraterritorial exercise of law enforcement that the government advocates in the Microsoft case imposes its own set of costs: it exacerbates data localization movements (the Balkanization of the Internet into multiple closed-off systems protected from the extraterritorial reach of foreign-based ISPs, with costs to the efficiently and effectiveness of the

Internet) and thereby undercuts U.S. business interests and also risks putting ISPs in an impossible bind—forcing them to choose between violating the laws of the requesting state or state where the data is stored.[9] Such an approach also makes it hard to object when another country—say China or Russia—seeks to compel the foreign-based subsidiary of a U.S.-based Internet service provider (ISP) to turn over emails and other data stored in the United States, including data of U.S. citizens. Thus, while this article recognizes, and in fact embraces, the need for new norms and procedures in response to the cross-border data flows, it argues that this is not something that should be unilaterally imposed, but built up over time, based on sovereign nation buy-in and consent.

This article fills an important gap in the literature. While there was a surge of literature in 1990s on the effect of a borderless Internet on sovereignty, the literature was primarily focused on the e-commerce issues that were emerging at the time—issues that were largely resolved through the harmonization of business practices.[10] By comparison, relatively little attention has been focused on the constitutional and sovereign interest implicated when it is the government that is reaching—or sending it agents—across borders to search and seize. Orin Kerr offers perhaps the most sustained attention to the issue, but he does so with a particular focus on border searches and with the goal of maintaining the territorial-based distinctions of the Fourth Amendment.[11] I, by contrast, argue that data challenges territoriality doctrine at its core, requiring us to re-think—and in some cases reject—the territorial-based distinctions as they apply to search and seizure of digital data.

I. TERRITORIAL PRESUMPTIONS

[9] *See, infra,* Part III(C). To be sure, such a conflict of laws is not unique to data. But it is something to be avoided when possible, and at a minimum is a cost that ought to be considered when considering the best approach going forward.

[10] *See, e.g.,* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367, 1375 (1996); Peter Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet,* 153 U. PENN. L. REV. 1975 (2005); JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2008). There is, of course, also a wealth of literature on the related issues regarding the relationship between new technology and privacy. *See, e.g.,* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014) [hereinafter Kerr, *The Next Generation*]; David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY (2012); Katharine Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008); William Banks, *Programmatic Surveillance and FISA – Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010) Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004). But the literature tends to avoid any sustained discussion of territorial-based considerations.

[11] Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015) [hereinafter Kerr, *The Global Internet*].

The increasing interconnectedness of our world has prompted renewed attention to territorial presumptions in law, their validity, and their effect. In a variety of contexts, both U.S. federal courts and the executive branch have sought to define and limit geographic reach of statutes, constitutional provisions, and international law treaty obligations. With some notable exceptions—including the Supreme Court's ruling in *Boumediene v Bush*[12] that the Suspension Clause extends to Guantánamo Bay—the recent trend has been one of entrenchment, with territorial-based presumptions waxing, not waning. For example, just four years ago, the Supreme Court upended longstanding assumptions about the reach of U.S. securities law in order to fortify the presumption against the extraterritorial application of statutory law.[13] This was followed by the Court's unanimous application of the same presumption to limit the extraterritorial reach of the Alien Tort Claims Act.[14] Meanwhile, the administration has recently undertaken its own searching inquiry into the geographic reach of key international law obligations, rejecting arguments that the International Covenant on Civil and Political Rights has extraterritorial application.[15] While the administration has sought, in the context of foreign intelligence surveillance and targeted uses of lethal force, to extend certain protections to non-resident aliens, it has done so as a matter of *policy*, not law.[16] The law continues to depend on a complicated set of territorial presumptions and applications—all of which depend at their core on the ability to define the

[12] 553 U.S. 723 (2008).

[13] Morrison v. Nat'l Austl. Bank Ltd, 561 U.S. 247 (2010).

[14] *See* Kiobel v. Royal Dutch Petroleum, 133 S. Ct. 1659 (2013). For interesting commentary, *see* Louise Weinberg, *What We Don't Talk About When We Talk About Extraterritoriality:* Kiobel *and the Conflict of Laws*, 99 CORNELL L. REV. 1471 (2014); Sarah Cleveland, *The* Kiobel *Presumption and Extraterritoriality*, 52 COLUM. J. TRANSAT'L L. 8 (2013).

[15] *See* Charlie Savage, *U.S., Rebuffing U.N., Maintains Stance That Rights Treaty Does Not Apply Abroad*, NY TIMES, March 14, 2014, at A12; Office of the Legal Adviser, Memorandum Opinion on the Geographic Scope of the Covenant on Civil and Political Rights, Oct. 19, 2010, *available at* http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf. *Cf.* Statement by NSC Spokesperson Bernadette Meehan on the U.S. Presentation to the Committee Against Torture, Office of the Press Secretary, The White House (Nov. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-presentation-committee-a (announcing the administration's conclusion that Article 16 of the Convention Against Torture, which prohibits cruel, inhuman, or degrading treatment, has extraterritorial application in any place that the "U.S. government controls as a governmental entity.")

[16] *See, e.g.,* The White House, *Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities*, May 23, 2013, http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism; Presidential Policy Directive--Signals Intelligence Activities (Jan. 17, 2014) [hereinafter PPD-28], § 4, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

relevant "here" and "there" and a determination that the "here" and "there" matter.[17]

This section sets the stage, describing key constitutional, statutory, and international law-based presumptions of territoriality that are embedded in the Fourth Amendment, statutory surveillance scheme, and warrant jurisdiction, as well as their application in specific cases. As the following highlights, the rules depend on two critical premises: first, that U.S. citizens and others with substantial connections to the United States are, as a matter of both constitutional law and policy preferences, entitled to greater privacy protections than non-citizens who lack substantial connections to the United States; and second, that respect of other states' sovereignty, concerns about international comity, and practical impediments to extraterritorial law enforcement actions, prohibit the issuance of extraterritorial warrants. Case law and commentary also have long assumed—generally without analysis—that the locus for assessing territoriality is that of the person or property being searched or seized. Cases involving compelled process pursuant to the government's subpoena power—along with the lower courts' opinions in the Microsoft case—provide some of the few examples to the contrary.[18]

A. THE TERRITORIAL FOURTH AMENDMENT

Until the 1950s, it was widely assumed that the Bill of Rights did not apply outside the nation's territorial borders, even when the United States was acting upon its own citizens.[19] Under the then-prevalent territorial understanding of the Constitution's reach, constitutional rights had full effect within the nation's borders, but generally not elsewhere.[20] In fact, even as the United States acquired new lands, only those territories that were "incorporated" within the United States (those destined for statehood) were protected by the entirety of the Bill of Rights. So-called "unincorporated" territories were protected by "fundamental" rights only.[21]

---

[17] *Cf.* Morrison, 561 U.S. at 266 (grappling with the question as to which conduct mattered for purposes of applying the territorial presumption)

[18] *See, e.g., In re* Grand Jury Proceedings Bank of Nova Scotia, 740 F.2d 817 (11th Cir. 1984); Marc Rich & Co., A.G. v. United States, 707 F.2d 663 (2d Cir. 1983).

[19] *See In re* Ross, 140 U.S. 453 (1891) (holding that constitutional rights protections did not apply in the prosecution of a capital crime by a U.S. consul in Japan). Conversely, actions taken within the U.S. were generally deemed covered by the constitution's protections, irrespective of the target of the action. *Cf.,* Sardino v. Fed. Reserve Bank of N.Y., 361 F.2d 106, 111 (2d Cir. 1966) (Friendly, J.) ("[T]he Government's [argument] that 'The Constitution of the United States confers no rights on non-resident aliens' is so patently erroneous in a case involving property in the United States that we are surprised it was made.")

[20] *See, e.g.*, Gerald L. Neuman, *Whose Constitution?,* 100 YALE L. J. 909, 918-19 (1990); KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG?: THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW (2001). *But see* J. Andrew Kent, *A Textual and Historical Case Against a Global Constitution*, 95 GEO. L.J. 463, 494-97 (describing exceptions to strict territoriality prior to 1957).

[21] Territories destined for statehood were deemed "incorporated" into the United States, whereas territories that were not slated to become states were "unincorporated" and "not a

By 1957, the territorial limits of the Constitution's reach began to crumble, at least as applied to U.S. citizens. After initially ruling—consistent with long-standing doctrine—that citizen-dependents of service members overseas were not entitled to the rights to a jury found in the Fifth and Sixth Amendments, the Supreme Court granted a rehearing and reversed itself the following term.[22] In *Reid v. Covert*, Justice Black wrote for a plurality of four:

> [W]e reject the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights. The United States is entirely a creature of the Constitution. . . . It can only act in accordance with all the limitations imposed by the Constitution.[23]

Justices Harlan and Frankfurter concurred, albeit on narrower grounds focused on the facts at hand—the trial of citizen-dependents for capital offenses.[24]

At the time, a number of scholars proclaimed, or at least advocated for, a new era of constitutional universalism, in which the government would be bound by the Bill of Rights, regardless of both where it was acting (Black's argument in *Reid*), or upon whom it was acting (the universalist addition).[25] But in its 1990 ruling in *U.S. v. Verdugo-Urquidez*,[26] the Supreme Court rejected the universalist approach and instead laid the groundwork for the two-part fixation with location and identity as determinative of the scope of Fourth Amendment rights.

The case involved a warrantless and extraterritorial search by U.S. agents of the Mexican residences of captured drug lord, Rene Verdugo-Urquidez, who was in U.S. custody in California at the time of the search. Although both the district court and Ninth Circuit ruled that the search violated the Fourth Amendment, a fractured Supreme Court reversed. Justice Rehnquist—on behalf of himself and Justices White, O'Connor, and Scalia—described the Fourth Amendment's reference to "the people" as a term of art referring to the "class of persons who are part of a national community or who have otherwise developed sufficient connection with

---

part of the United States." Downes v. Bidwell, 182 U.S. 244, 287 (1901); *id.* at 342 (White, J., concurring). *See* Christina Duffy Barnett, *A Convenient Constitution? Extraterritoriality After* Boumediene, 109 COLUM. L. REV. 973 (2009).

[22] *See* Kinsella v. Krueger, 351 U.S. 470 (1956); Reid v. Covert, 351 U.S 387 (1956); (*reh'g granted* in both cases, Reid v. Covert, 352 U.S. 901 (1956); *overruled,* Reid v. Covert, 354 U.S. 1 (1957)).

[23] Reid v. Covert, 354 U.S. 1, 5-6 (1957).

[24] Three years later, Justices Harlan and Frankfurter dissented from a ruling extending the jury trial protections to citizen-dependents in a *non*-capital case. Kinsella v. United States *ex rel.* Singleton, 361 U.S. 234, 249 (1960) (Harlan & Frankfurter, JJ., dissenting)

[25] *See, e.g.* Louis Henkin, *The Constitution as Compact and as Conscience: Individual Rights Abroad and At Our Gates*, 27 WM. & MARY L. REV. 11, 34 (1985); Jules Lobel, *Here and There: The Constitution Abroad,* 83 AM. J. INT'L L. 871, 879 (1989) ("The separation of the international from the domestic legal order, upon which the denial of constitutional rights to aliens is based, is breaking down."); *cf.* Paul B. Stephan III, *Constitutional Limits on the Struggle against International Terrorism: Revisiting the Rights of Overseas Aliens*, 19 CONN. L. REV. 831 (1987) (opposing the universalist push).

[26] 494 U.S. 259 (1990).

this country to be considered part of that community."[27] The court thus adopted what Professor Gerald Neuman labeled a "membership" theory of constitutional rights.[28] Verdugo-Urquidez needed to have developed "sufficient connections" to the United States in order for the Fourth Amendment to apply; two days in U.S. jail did not suffice.[29]

Justice Kennedy provided the critical fifth vote. But while purporting to join Rehnquist's opinion, he repudiated the central theory. Specifically, Kennedy rejected the assertion that the Fourth Amendment's reference to "the people" was a term of art exclusively referring to a class of U.S. citizens and those with sufficient connections to the United States. Kennedy instead argued that the reference to "the people" was of unclear import and could just as readily "be interpreted to underscore the importance of the right, rather than to restrict the category of persons who may assert it."[30] That said, he too rejected a universalist approach to constitutional rights—emphasizing "the undoubted proposition that the Constitution does not create, nor do general principles of law create, any juridical relation between our country and some undefined, limitless class of noncitizens who are beyond our borders."[31] Kennedy instead advocated a pragmatic approach to the extraterritorial application of constitutional rights, drawing on Justice Harlan's 1957 concurrence in *Reid*. According to Kennedy, it would be "impractical and anomalous" to enforce the Fourth Amendment's warrant requirement in the context of a foreign search of a non-resident alien; thus, the warrantless search of Verdugo-Urquidez's Mexican residences did not violate the Fourth Amendment.[32]

---

[27] *Id.* at 265 (1990) (plurality opinion).

[28] *See* GERALD NEUMAN, STRANGERS TO THE CONSTITUTION (1996), at 6-7 (defining the membership theory to mean that only those with sufficient connections to the United States are entitled to constitutional rights protections). *See also* Chimene I. Keitner, *Rights Beyond Borders,* 36 YALE J. INT'L L. 555 (2011) (defining this approach as the compact model).

[29] Verdugo-Urquidez, 494 U.S. at 271-72. For a fuller analysis of the *Verdugo-Urquidez* ruling and its implications, see Jennifer Daskal, *Transnational Seizures: The Constitution and Criminal Procedure Abroad*, in CONSTITUTIONALISM ACROSS BORDERS IN THE STRUGGLE AGAINST TERRORISM (Federico Fabbrini & Vicki Jackson eds.) (forthcoming 2015).

[30] 494 U.S. at 276. *See also* United States v. Verdugo-Urquidez, 856 F.2d 1214, 1223 (9th Cir. 1998) (*rev'd*, 494 U.S. 259 (1990)) (arguing that the Framers' primary concern was that of protecting natural rights and thereby rejecting the attempt to restrict the application of the Fourth Amendment to any special class of people).

[31] 494 U.S. at 275.

[32] Notably, Kennedy focused his analysis on the impracticability of applying the *warrant* requirement to an extraterritorial search or seizure, saying nothing about the feasibility and practicability of applying the Fourth Amendment's reasonableness requirement to extraterritorial searches and seizures. Moreover, he simply assumed, without analysis, that issuance of a warrant would provide the affirmative authorization to search -- something that U.S. courts lacked jurisdiction to authorize if the target of the search was located extraterritorially. He thus failed to consider the possibility of a warrant requirement that served the limited—but critically important—purpose of ensuring that the search comported with U.S. constitutional protections, without also authorizing U.S. agents to take action abroad.

Despite the splintered analysis, *Verdugo-Urquidez* now stands for the proposition that the United States is freed from the constraints of the Fourth Amendment when it searches or seizes a non-citizen outside the United States, unless the non-citizen has developed substantial, voluntary connections with the United States.[33] Conversely, while the Supreme Court has not squarely addressed the question of *citizens'* Fourth Amendment rights abroad, lower courts have concluded that U.S. actions against citizens are covered by the Amendment's protections, but that the reasonableness test—not the warrant requirement—apply.[34]

Thus has emerged a two-step decision tree: First, where does the search or seizure take place? If in the United States, the Fourth Amendment applies.[35] If outside the United States, then turn to the question of identity: Is the target of the search or seizure a U.S. citizen or alien with substantial voluntary connections to the United States? If yes, then the Fourth amendment applies, and the test is one of reasonableness. If, on the other hand, the target is a non-citizen lacking substantial connections to the United States, the Fourth Amendment does not apply, and the government need not abide by even the minimal requirement of reasonableness with respect to actions directed at the target.

This same basic framework has been relied on to determine the extraterritorial reach of the Fifth Amendment, as well as a range of other constitutional rights obligations. And while the 2008 ruling in *Boumediene v. Bush*, in which the Supreme Court held that the Suspension Clause protected aliens at Guantanamo Bay, precipitated new proclamations of an emergent

---

[33] Lower courts have adopted differing interpretations of what constitutes sufficient contact to trigger the Fourth Amendment's application, and the Supreme Court to date has failed to clarify. *Compare*, for example, Martinez-Aguero v. Gonzalez, 459 F.3d 618 (5th Cir. 2006) (illegal alien entitled to Fourth Amendment protections) *with* United States v. Esparza–Mendoza, 265 F.Supp.2d 1254, 1271 (D.Utah 2003) (ruling that previously deported alien felons do not have a "sufficient connection to this country" to be protected by the Fourth Amendment).

[34] *See, e.g.,* United States v. Stokes, 726 F.3d 880 (7th Cir. 2013) (applying a reasonableness test to the extraterritorial search of a citizen's property); In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167 (2d Cir. 2008); *see also* United States v. Peterson, 812 F.2d 486 (9th Cir. 1987) (also applying a reasonableness test, but adopting a slightly different definition of reasonableness that depends on adherence to foreign law). *Cf. In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA. Ct. Rev. 2008) (suggesting that the warrant clause applies, but is subject to a foreign intelligence exception).

[35] Some courts have relied on Justice Rehnquist's language in *Verdugo-Urquidez* to suggest that even within the United States, only U.S. citizens and aliens with substantial voluntary connections are entitled to the Fourth amendment protections. *See, e.g.,* United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1273 (N.D. Utah 2003) (holding that a previously deported felon present in the United States is not entitled to Fourth Amendment protections); *cf.* United States v. Carpio-Leon, 701 F.3d 974 (4th Cir. 2012) (relying in part, on *Verdugo*, to conclude that illegal aliens are not entitled to Second Amendment rights). But while Rehnquist's language opens up the possibility, this is a minority view. Moreover, Rehnquist himself describes the holding as addressing the *extraterritorial* application of Fourth amendment rights.

constitutional universalism, this has not yet materialized.[36] To the contrary, lower courts have largely restricted *Boumediene* as applying to the Suspension Clause and possibly other so-called "structural" provisions of the Constitution, such as the Ex Post Facto Clause. Courts continue to rely on *Verdugo-Urquidez* as a basis for concluding that non-citizens without substantial connections to the United States lack Fourth Amendment and other so-called "individual" rights.[37] In fact, it even remains unsettled as to whether basic rights protections—as distinct from the Suspension Clause—apply to the Guantánamo detainees.[38]

But this is not the only way to think about the Fourth Amendment. As described above, Justice Kennedy, for example, suggests that the term "the people" emphasizes the importance of the right, rather than strictly limit its application to a certain class. Professor David Gray, also relying on the term "the people," persuasively suggests that the term was selected to emphasize its collective importance to all of us. According to Gray, the Fourth Amendment is about protecting the collective—that when an

---

[36] *See, e.g.,* Sarah L. Cleveland, *Embedded International Law and the Constitution Abroad,* 110 COLUM. L. REV. 225, 230 (2010) (suggesting that *Boumediene* marked a sea change in U.S. jurisprudence); Gerald L. Neuman*, The Extraterritorial Constitution After Boumediene v. Bush*, 82 S. CAL. L. REV. 259, 290 (2009) (describing the Boumediene opinion as a "repudiation of the Verdugo-Urquidez plurality"); David D. Cole, *Rights Over Borders: Transnational Constitutionalism and Guantánamo Bay*, 2008 CATO SUP. CT REV. 47, 61 (describing Supreme Court as having rejected "outmoded claims about sovereignty, territoriality, and rights"). For a similar perspective from those critical of what *Boumediene* might portend, *see* Andrew Kent, *Boumediene, Munaf, and the Supreme Court's Misreading of the Insular Cases,* 97 IOWA L. REV. 101, 103 (2011) (pronouncing *Boumediene* "an enormously significant inflection point in U.S. constitutional law'); Eric Posner, *Boumediene and the Uncertain March of Judicial Cosmopolitanism*, 2008 CATO SUP. CT REV. 23. 24 (warning of an emerging "judicial cosmopolitanism").

[37] *See, e.g.*, Hernandez v. United States, 11-50792 (5th Cir. Apr. 24, 2015) (en banc); United States v. Emmanuel, 565 F. 3d 1324 (11th Cir. 2009); Rasul v. Myers, 563 F.3d 527, 529 (D.C. Cir. 2009) (stating that "the Court in *Boumediene* disclaimed any intention to disturb existing law governing the extraterritorial reach of any constitutional provisions, other than the Suspension Clause"). *See also* United States v. Ali, 71 M.J. 256 (C.A.A.F. 2012) (holding that an alien working as a civilian contractor in Iraq is not entitled to jury trial rights); Ibrahim v. Dep't of Homeland Sec., 669 F.3d 983, 997 (9th Cir. 2012) (ruling that non-citizen could raise First and Fifth Amendment claims only because she had developed "substantial, voluntary connections" with the United States); Atamirzayeva v. United States, 524 F.3d 1320 (Fed. Cir. 2008) (concluding that alien lacking sufficient connection to the United States was not entitled to relief under the Fifth Amendment Takings Clause).

[38] *See, e.g.,* Kiyemba v. Obama, 555 F.3d 1022, 1026 (D.C. Cir. 2009) (holding that Guantánamo detainees cannot invoke the Due Process Clause), *vacated*, 559 U.S. 131 (per curiam), *modified*, 605 F.3d 1046 (D.C. Cir. 2010) (per curiam); United States v. Hamdan, 801 F. Supp. 2d 1247, 1318 (C.M.C.R. 2011) (rev'd on other grounds, Hamdan v. United States, 696 F.3d 1238 (2012)). *See also* Kal Raustiala, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 244-45 (2009) ("Structural provisions, such as bans on title of nobility, are arguably different [from individual-rights provisions]. Because they determine the scope of federal power, they apply everywhere the federal government acts."); Boumediene v. Bush, 476 F.3d 981, 995-98 (D.C. Cir. 2007) (Rogers, J., dissenting), *rev'd*, 553 U.S. 723 (2008) (distinguishing between structural and individual rights provisions of the U.S. Constitution).

individual claims a Fourth Amendment right he stands in for the rest of us.[39] The import of Gray's insight depends in part on the definition of the term "the people," which, as history reminds us, can be defined narrowly or broadly.[40] But even assuming a definition "the people" that covers only citizens and others with sufficient connections to the United States, Gray's approach moves us away from the individualist focus on the particular target of the government action—*i.e.,* the idea that Jack has not suffered a Fourth Amendment violation if evidence against him was illegally obtained targeting Jill, or anyone else other than him. Under Gray's approach, Jack—as a representative of "the people"—could claim a Fourth Amendment violation any time the government's impermissible activity implicated him.[41] And this is so regardless of the identity the particular, intended target of the state's action—such as, for example, when the government targets a non-U.S. person in communication with a U.S. citizen.

The *Verdugo-Urquidez* case highlights yet another interesting aspect of Fourth Amendment doctrine—namely, the long-standing assumption that the first step of territoriality inquiry turns on the location of the property being searched, rather than the location of either the target of the search or the agent doing the search. The search of Mr. Verdugo-Urquidez's residence took place in Mexico while Mr. Verdugo-Urquidez was being held in the United States. Yet, it was simply assumed, without discussion, that the search was extraterritorial, not territorial. What mattered was the location of the property being searched, not the location of the person whose property was being searched.[42] Other cases buttress this presumption that the location of the property searched is what matters. In *Riley v. California*,[43] for example, the Supreme Court, in holding that the warrantless search of a cell phone could not be justified as a search incident to arrest, highlighted the possibility that agents might be remotely accessing data stored in the cloud. As the Court put it, this would be akin to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[44] Again, the Court's primary concern was the location of the data being searched, not the location of the device used to access the data or the agent doing the searching. Similarly, in *Kyllo v. United States*,[45] agents standing on a public street used a thermal imaging device to detect heat levels emanating from inside Mr. Kyllo's home. The Court

---

[39] *See* David Gray, *The Fourth Amendment as Rights, Part I: The Warrant Requirement*, at 20-21 (forthcoming) (on file with author).

[40] *See, e.g.,* Dred Scott v. Sandford, 60 U.S. (19 How.) 393 (1856).

[41] In fact, Gray seems to want to go even a step farther, suggesting perhaps that Jack need not have suffered an injury in fact in order to bring such a claim. I am not persuaded by that point.

[42] *Cf.* R. . v. Hape, 2007 SCC 26, para. 69, [2007] (holding that the Canadian Charter of Rights and Freedom did not apply to the extraterritorial search by Canadian officials of a Canadian citizen who was being prosecuted in Canada).

[43] 134 S. Ct. 2473 (2014).

[44] *Id.*

[45] 533 U.S. 27 (2001).

deemed this a search of the *home*, even though both the thermal imaging device and the agents involved were outside the physical home.

B. TERRITORIAL-BASED SURVEILLANCE AUTHORITIES

The statutory and regulatory regime governing foreign intelligence surveillance tracks Fourth Amendment doctrine, with its strong emphasis on location and nationality as determinative of the rules that apply.[46] As initially passed in 1978, the Foreign Intelligence Surveillance Act (FISA) regulated the collection of electronic communications for foreign intelligence purposes.[47] It focused specifically on surveillance targeted at persons based in the United States, as well as territorial-based acquisitions of international wire communications when the targeted communication is to or from a person within the United States.[48] With a few narrow exceptions, all such collection required a warrant issued by the Foreign Intelligence Surveillance Court, based on a finding that the target was a "foreign power" or an "agent of a foreign power."[49] The warrant requirement applied to citizens and non-citizens alike, albeit with heightened standards governing the targeting of a "U.S. person"—*i.e.,* a U.S. citizen or legal permanent resident.[50] Meanwhile, extraterritorial surveillance, by which I refer to collection of data located outside of the United States that is targeting persons located outside the United States, was left to the Executive Branch, even when the targets were U.S. citizens.[51] Since 1982, such extraterritorial surveillance has been governed by Executive Order 12,333.[52]

At its inception, FISA's focus was the protection of U.S. persons, defined to include citizens and legal permanent residents. At the time of passage, some members of Congress argued that the warrant requirement should cover U.S. persons only, and not applied to others, such as resident aliens that were not legal permanent residents and non-resident aliens whose

---

[46] A quick word on terminology: The statute refers to the "acquisition" of electronic communications to describe the "collection" of such information. I use these terms interchangeably.

[47] FISA regulates electronic surveillance targeting foreign powers and agents of foreign powers, physical searches targeting foreign powers and agents of foreign powers, pen/trap surveillance, and judicially compelled productions of tangible things. This article is primarily focused on electronic surveillance.

[48] *See* 50 U.S.C. § 1801(f)(4)(2008). For an excellent and detailed explanation of FISA's scope, see DAVID KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS, §§ 7:2-7:16 (2012) [hereinafter KRIS & WILSON, NSIP].

[49] 50 U.S.C. § 1805(a)(2)(A) (2008); *see also id.* § 1802 (defining the circumstances in which the executive branch could authorize territorial electronic surveillance without a court order).

[50] 50 U.S.C. § 1801(i)(2008). The definition of "U.S. persons" also includes unincorporated associations in which a "substantial number" of members are U.S. citizens or legal permanent residents, and most corporations incorporated in the United States. *Id.*

[51] This is not the only way to define extraterritorial surveillance. One could, for example, consider all collection that takes place outside the United States to be extraterritorial, regardless of whether the target is in the United States or outside the nation's borders.

[52] Exec. Order 12,333, 3 C.F.R. 206 (1982); KRIS & WILSON, NSIP, *supra* note 46, at § 4:2.

communications were covered by FISA when the collection took place in the United States. But Congress ultimately decided to apply the warrant requirement to all such collection. The House Intelligence Committee emphasized that a broad warrant requirement was imposed

> not. . . primarily to protect such persons but rather to protect U.S. citizens who may be involved with them and to ensure that the safeguards inherent in a judicial warrant cannot be avoided by a determination as to a person's citizenship.[53]

The quote exemplifies the 1978 Congressional understanding of two important facts: First, the acquisition of non-U.S. person communications could yield the incidental collection of U.S. person information. The aptness of the insight has only increased over time. When Congress passed FISA in 1978, most communications were truly domestic—between two or more U.S.-based users, and involving data that did not leave the territorial boundaries of the United States. This is no longer true. Now the Internet is truly global, with communications transiting in and out of the nation's boundaries with regularity, and often involving at least one foreign-based sender or recipient.[54] When the government acquires communications of non-U.S. persons, whether located territorially or extraterritorially, it also risks scooping up a significant amount of U.S. person data.

Second, a universally applicable warrant requirement provided a critical protection against erroneous citizenship determinations that would otherwise result in the warrantless surveillance of U.S. citizens. Congress demanded a warrant for the acquisition of non-US person information, not because it was interested in protecting non-U.S. persons' privacy, but as a means of protecting the U.S. persons that were the focus of its concern.

As passed in 1978, FISA did not extend to the extraterritorial surveillance of U.S. persons located outside the United States—something that was left to the executive branch, but that Congress committed to addressing in due course.[55] Thirty years later, Congress finally took up the issue. The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA) extended FISA's warrant requirement to cover the extraterritorial surveillance of a U.S. person located outside the United States, thereby bringing the extraterritorial surveillance of U.S. person under FISA's statutory scheme.[56] At the same time, Congress eliminated the

---

[53] HOUSE PERMANENT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, H.R. REP. No. 1283, pt. I, 95th Cong., 2d Sess. (1978) [hereinafter House FISA Report] at 26, *available at* http://fas.org/irp/agency/doj/fisa/hspci1978.pdf (emphasis added).

[54] *See, e.g.,* Kerr, *The Next Generation Communications Privacy Act*, *supra* note 10, at 404-06 (describing the evolution of the Internet from the early 1980s to 2014).

[55] House FISA Report, *supra* note 51, at 28.

[56] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA), Pub. L. No. 110-261, 122 Stat. 2436 (2008) §§ 703, 704 (codified at 50 U.S.C. §§ 1881b; 1881c). In contrast to FISA as passed in 1978, protections for U.S. person targets does not appear to be key the motivating force behind the 2008 legislation. In fact, protections for U.S. persons located extraterritorially were first added as an amendment to then-pending version

warrant and probable cause requirement for the territorial acquisition of non-U.S. person targets located extraterritorially—thereby ignoring the risk of intermingled data and erroneous targeting decisions.

In broad-brush strokes, territorial-based presumptions now operate along two axis: first, the targeting of *persons* located inside the U.S., as well as U.S. citizens and legal permanent residents wherever they are located, is subject to more rigorous standards and procedural protections than the targeting of non-citizens located outside the U.S., and second, collection of *data* located within the United States is generally subject to heightened restrictions compared to collection that takes place outside the United States. The scheme thus tracks the territorial-based line drawing of the Fourth Amendment, albeit with an added focus on *target* location in addition to *property* location and target identity.

More specifically, the Foreign Intelligence Surveillance Court (FISC) must approve the targeted electronic surveillance of all persons in the United States as well as U.S. persons outside the United States, based on a probable cause finding that the requisite targeting standard has been met—that the target is a "foreign power," "agent of a foreign power," or for U.S. persons located outside the United States, "employee or officer of a foreign power" (an addition meant to cover those work for foreign government or a foreign government-owned company).[57] Conversely, electronic surveillance targeting non-U.S. located outside the United States—what is known as "702" surveillance based on the statutory numbering of the FAA—is now permitted without a warrant, finding of probable cause, or even a requirement that the target be a foreign power, agent or employee of a foreign power.[58] Rather, the Attorney General (AG) and the Director of National Intelligence (DNI)—not the FISC—jointly authorize the targeting of non-citizens "reasonably believed to be located outside the United States to acquire foreign intelligence information," subject to certain statutory

---

of the legislation in October 2007, adopted by the Senate Intelligence Committee by a fairly narrow vote of 9-6. See Jonathan W. Glannon, *From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations,* 6 J. NAT'L SEC. L. & & POL'Y 59, 80-85 (2012) (tracking the legislative history of U.S. person provisions in the FAA)

[57] When surveillance is targeting persons in the United States (and thereby requires as warrant based on a finding of probable cause), rules also vary depending on whether the target is a U.S. person or non-U.S. person. The definition of "agent of a foreign power" is broader for non-U.S. persons than U.S. persons, *see* 50 USC § 1801(b)(2008); the type of information that can be sought is broader for non-U.S. persons than U.S. persons, *see* 50 U.S.C. § 1801(e)(2008); 50 U.S.C. § 180(a)(6)(B)(2008); and the duration of permitted collection is longer for non-U.S. persons, *see* 50 USC § 1805(d)(1)(2008). Required minimization procedures, which limit the acquisition and dissemination of non-relevant information, apply to U.S. persons only, *see* 50 U.S.C. § 1801(h)(2008). That said, Presidential Policy Directive 28, issued January 17, 2014, stated that as a matter of *policy*, intelligence agencies must eliminate, where possible, differences in the dissemination and retention rules governing U.S. person and non-U.S. person information. *See* PPD-28, *supra* note 17, § 5; *see* discussion, *infra*, notes __.

[58] *See* 50 USC §1881a. *See* Laura Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y __(forthcoming 2015).

limitations.[59] The FISC's role is limited to approving minimization procedures, designed to limit the acquisition, retention, and dissemination of information involving U.S. persons, and reviewing a joint AG and DNI "certification" attesting that a significant purpose of the collection is to acquire foreign intelligence information and that all other statutory requirements are being met.[60]

In practice, targeting under 702 is initiated when a National Security Agency (NSA) analyst learns that a particular person may possess or receive the kind of foreign intelligence information covered within one of the approved certifications. (The FBI or CIA can nominate targets, but it is the NSA that makes the ultimate targeting decision.) The analyst then engages in a "foreignness" determination—namely a totality of the circumstances determination that the target is a non-U.S. person "reasonably believed" to be located outside the U.S.[61] Because a target's identity is not always known, the NSA applies certain presumptions. When a target's location is either unknown or known to be outside the United States, the target is treated as a non-U.S. person absent a "reasonable belief" that such person is a U.S. person.[62] These, however, are hardly foolproof presumptions, as there are a host of reasons why a U.S. person might be temporarily or permanently located outside of the United States. That said, the Department of Justice's reporting suggests that the error rate is quite low—just 0.4% in a review of 2011 data. Of course, the report only catches known errors and does not tell us anything about unknown errors.[63] Moreover, even a low rate or error can yield high numbers of erroneous "foreignness" assessments, given the sheer quantity of data that is currently being collected.

---

[59] 50 U.S.C. § 1881a(a).

[60] 50 U.S.C. § 1881a(g) (describing certification requirement). Approved certifications reportedly authorize the acquisition of information concerning international terrorism and weapons of mass destruction, and possibly other topics as well. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Act* (July 2, 2014) at 25 n. 71 [hereinafter PCLOB 702 Report], http://www.pclob.gov/library/702-Report.pdf.

[61] PCLOB 702 Report, *supra* note 58, at 42-44.

[62] MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, AS AMENDED, Oct. 31, 2011 at § 2(k)(2), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf [hereinafter 2011 MINIMIZATION PROCEDURES]. According to Raj De, General Counsel of the NSA, any "contrary" evidence must be considered, but the ultimate test is one of a "totality of the circumstances." See Hearing Transcript, at 40-41, http://www.pclob.gov/library/20140319-Transcript.pdf; PCLOB 702 Report at 4, *supra* note 58, Donohue, *supra* note 56 (describing foreignness determination under 702).

[63] PCLOB 702 Report, *supra* note 58, at 44. These statistics do not include data obtained pursuant to Executive Order 12,333, and do not include instances in which DOJ correctly determined that the target was a non-U.S. person located outside the United States, but the target subsequently traveled to the United States and 702 collection nonetheless (and impermissibly) continued.

Once a target is identified, NSA then approves "selectors" associated with the target—*i.e.* an email account such as johnsmith@gmail.com used by the target. In NSA speak, this is known as the "tasked selector." It is possible to have multiple selectors associated with each target.

There are reportedly two main collection programs pursuant to 702: PRISM collection and upstream collection. Pursuant to PRISM collection, the government sends approved selectors, such as emails associated with targeted persons, to an electronic service provider. The electronic service provider is compelled to turn over all communications sent to or from the selector to the NSA.[64] As of mid-2011, approximately 90 percent of all communications collected pursuant to 702 was obtained through PRISM—yielding an estimated 227.5 million Internet communications each year.[65] Upstream collection, by contrast, occurs on the Internet and telecommunications backbone, the fiber optic cables over which Internet communications travel. Transactions are first screened to eliminate "domestic communications," as required by the statute, and defined to include transactions where both the sender and all recipients are located within the United States, and then the transactions are screened to determine whether they contain the tasked selector.

There are three points worth noting about upstream collection. First, as just described, the screen for domestic communications requires NSA to eliminate only those communications in which the sender and recipients are "known" to be located in the United States. In many cases the location of the sender and recipient will be unknown. Moreover, even if the filtering tools employed by the NSA operate with 100 percent accuracy, the definition of "domestic communications," as defined by statute, is quite narrow. It is limited to those communications in which the sender and *all* recipients are based in the United States. It does not include an email update sent to 30 friends and family members, as long as one of the 30 was outside the United States at the time he or she received the communications.

Second, such collection does not just yield information that is "to" or "from" a tasked selector, but also yields communications that are "about" a selector—*i.e.*, communications in which the target is referenced but the target is neither the sender nor recipient of the communications. This means that even though 702 collection is directed at non-U.S. persons located outside the United States, NSA can collect a U.S. person-to-U.S. person communication as long as one of the parties to the communication

[64] PCLOB 702 Report, *supra* note 58, at 7. The NSA receives all data collected through PRISM, and the CIA and FBI each receive a portion of such data.

[65] Judge Bates Opinion, *Redacted*, 2011 WL 10945618, at *10 (FISA Ct. Oct. 3, 2011) [hereinafter Bates 2011 Opinion] (referring to the fact that NSA acquires "more than 250 million Internet communications each year pursuant to 702, 91% of which are obtained pursuant to what is known as PRISM collection"); PCLOB 702 Report, *supra* note 58, at 34 n. 119.

is outside the United States and the communication refers to (is "about") the tasked selector.

Third, as of 2011, up to 60 percent of upstream collection involved the acquisition of what are known as multiple communication transactions, defined as multiple discrete communications packaged together for the purpose of transiting the fiber-optic lines. As long as one of the discrete communications included in the transaction contains information "to," "from," or "about" the tasked selector, NSA acquires the entire multi-communication transaction, including other discrete communications that may not contain the selector.[66] As of 2011, NSA acquired approximately 26.5 million Internet transactions through upstream collection each year. This includes tens of thousands of communications that are not "to," "from," or "about" the tasked selector, but collected nonetheless.[67] It also includes the collection of tens of thousands of wholly domestic communications.[68] As Judge Bates, then-Chief Judge of the FISC, wrote in 2011, "NSA's acquisition of [multiple communication transactions] substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA's Section 702 collection."[69]

The executive branch also engages in a range of extraterritorial surveillance activities not regulated by FISA, but instead governed by Executive Order 12,333. Reports suggest that electronic surveillance pursuant to 12,333 is substantial, and presumably accounts for an even greater share of electronic surveillance activities than any equivalent surveillance conducted under the FISA or FAA authorities.[70] While warrantless targeting of U.S. person communications under 12,333 is prohibited in situations where a warrant would be required if the collection was being done by law enforcement agents in the United States,[71] reporting

---

[66] *See* PCLOB 702 Report, *supra* note 59, at 7.

[67] *See id.* at 134; Bates 2011 Opinion, *supra* note 63, at *15 ("By acquiring such MCTs [multi-communication transactions], NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector."); *but see id.* at * 10 (emphasizing that, given technological change, "it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.")

[68] *Id.* at *11 (describing an estimated 2,000 to 10,000 multiple communication transactions that include at least one wholly domestic communications, plus an estimated 46,000 single communication transactions that were not screened out as wholly domestic—when, example, a U.S.-based person uses a foreign server, making it appear as if the communication included at least one non-U.S.-based user).

[69] *See id.* at *25 (emphasizing that collection of tens of thousands of non-target, protected communications annually is a "*very* large number") (emphasis in original).

[70] *See, e.g.,* Alvaro Badoyo, *Executive Order 12,3333 and the Golden Rule*, JUST SECURITY (Oct. 9, 2014), http://justsecurity.org/16157/executive-order-12333-golden-number/; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule that lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

[71] *See* 50 U.S.C. § 1881c(a)(2); *see also* Jonathan W. Gannon, *From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad In Light of Recent Terrorism Prosecutions*, 6 J. NAT'L SEC. L. POL'Y 59 (2012).

suggests that large quantities of U.S. person information is being obtained nonetheless.[72] Of note, Executive Order 12,333 collection reportedly includes "vacuum cleaner" or "bulk" collection, pursuant to which the executive sweeps in all communications that transit particular cables, including communications that are to or from U.S. persons; Internet metadata collection;[73] and collection of address books and buddy lists of U.S. persons.[74] Such bulk collection is not deemed to target anyone, thus avoiding the prohibition on targeting U.S. persons. Other collection programs fall outside the prohibition on targeting U.S. persons on the grounds that such collection would not require a warrant if done for law enforcement purposes in the United States.

Thus, while FISA requires a warrant to conduct electronic surveillance of U.S. persons, in practice U.S. person information can be collected without a warrant in one of six situations: (1) if NSA errs in its foreignness determination, and targets a U.S. person believing that person to be a non-U.S. person; (2) when a U.S. person is in direct communication with a non-U.S. person target; (3) when, as permitted in the context of so-called "upstream" collection, the government targets communications "about" a non-U.S. person target, and a party to the "about" communication is a U.S. person; (4) when, also permitted as a part of upstream collections, the government collects a multi-communication transaction that includes discrete communications to or from U.S. persons that does not include information that is to, from, or about the target; (5) when the government, pursuant to Executive Order 12,333, engages in "vacuum cleaner" collection and therefore is not technically "targeting" anyone, yet collects all information that transits through a particular collection device; or (6) or as a result of extraterritorial surveillance activities that the executive branch concludes would not trigger a warrant requirement if carried out in the United States by law enforcement, thus freeing the government from the restrictions on the targeting of U.S. persons under EO 12,333. Categories 2-5 are all examples of "incidental collection," and likely account for the vast majority of acquired U.S. person information.

To sum up, the entire statutory framework for and executive branch regulation of foreign intelligence surveillance is premised on an assumption that persons located in the United States are entitled to greater privacy protections than those without, and that U.S. persons are entitled to greater privacy protections than non-U.S. persons. Yet, the scope of incidental collection raises questions about whether the scheme is providing adequate privacy protections for the U.S. persons it is designed to protect, at least at the collection stage. The intelligence community, in response, points to minimization rules that limit the retention, dissemination, and access to

[72] *See* Tye, *supra* note 68.

[73] *Id.*

[74] *See* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally,* WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html.

collected U.S. person data.[75] And minimization rules, if sufficiently robust, do in fact provide important privacy protections. But it is worth noting that minimization rules and other use restrictions have been given only scant attention by Congress to date. While Congress has mandated that minimization procedures be put in place, it has delegated all the key details to the executive branch. Meanwhile, it has made collection its central focus, legislating extensively on both the substantive standards and procedural requirements governing the acquisition of electronic data.

Thus, while never explicitly stated, Congress appears to be operating under the assumption that the collection itself poses a privacy intrusion – and potential harm - that needs to be regulated, even if only a consequentialist harm about how the information might be used in the future to chill speech or to shift the balance of power between the governed and the government.[76] To the extent that Congress, the public, and the courts remain concerned about, and seek to limit, the government's acquisition of U.S. person data, the current set of territorial and identity-based presumptions are providing insufficient protections. I return to this in Part III.

C. TERRITORIAL WARRANT AUTHORITY

Distinct from the territorial-based limits on the Constitution's warrant *requirement*, which reflect territorial and identity-based limits on the privacy protections owed by the U.S. government, there is a question as to the geographic reach of the court's warrant *authority,* an issue which implicates, among other things, questions of state sovereignty. The overarching rule is that the judiciary's warrant authority is territorially limited—a limit that is reflected in the Federal Rules of Criminal Procedure

---

[75] *See, e.g,* Office of the Director of National Intelligence, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28* (July 2014), http*://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf* (emphasizing the importance of limitations on the use, dissemination, and retention of collected data); United States Signals Intelligence Directive-18 (Jan. 25, 2011) (indicating that concerns raised by the collection of US person information is dealt with through minimization procedures), http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf / *see also* David Cole & Marty Lederman, *Data Mining, Section 215, and Regulation the Use of Stored Data: The Overlooked, but More Important Question About 215 Surveillance*, JUST SECURITY (Dec. 23, 2013), http://justsecurity.org/4932/review-group-intelligence-communications-technologies-bulk-data-collection-section-215/ (emphasizing the often overlooked importance of the "use" question).

[76] *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 488 (2006) (describing privacy as protecting against what he calls architectural harms—information gathering that creates a risk of future harm or that shifts the balance of power between the government and the governed and results in a chilling effect); *See also* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) (warning that "[t]he condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.").

(FRCP), relevant statutes, and a smattering of case law.[77] Under well-accepted principles of international law, State A can directly engage in law activities in State B only if it has State B's consent. As a result, judges are presumed to lack authority to unilaterally authorize extraterritorial searches and seizures.[78]

The following describes these territorial limits as applied to "ordinary" warrants issued pursuant to the Federal Rule of Criminal Procedure 41 (Rule 41), warrants issued under the Wiretap Act, which authorize real-time collection of electronic communications, and warrants issued on the Stored Communications Act, which authorize collection of, as the name suggests, stored communications. While the territorial presumption is clear, its application to the collection of data is not. Is the appropriate reference point the location of the data, the provider, or the government agent that is accessing the data, or possibly a combination of all three? As described below, there are not obvious answers, and the government has suggested different answers depending on the context and its preferred outcome.

(i) Rule 41

Rule 41 of the FRCP prescribes the authority of magistrate judges to issue a warrant authorizing a search or seizure. This authority is generally limited to property or persons within the district in which the magistrate works. Even in those limited situations, such as terrorism cases, in which judges are permitted to issue warrants authorizing out-of-district searches or seizures, such warrants are widely understood to be subject to territorial-based limitations.[79] In fact, the only instances in which a magistrate judge is explicitly authorized to issue a warrant with extraterritorial reach are limited to situations in which the property or person to be searched or seized is located in a U.S. territory, possession, or commonwealth; on the premises of a U.S. consular or diplomatic mission; or on the residence or land owned or leased by the United States and used by U.S. diplomats or consular

[77] *See, e.g.,* Restatement (Third) of Foreign Relations § 432(2) ("A state's law enforcement officer may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state"); United States v. Odeh, 552 F.3d 157, 166 (2d Cir. 2008) (noting that in *Verdugo-Urquidez* "seven justices of the Supreme Court endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches"); United States v. Barona, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) ("[F]oreign searches have neither been historically subject to the warrant procedure, nor could they be as a practical matter.").

[78] *See, e.g.*, JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW (8th ed.) 478-79 (2012); Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. OF INT'L LAW 345, 372 (2009) ("The exercise of enforcement jurisdiction in the territory of another state, without its consent, breaches the non-intervention principle . . . extraterritorial enforcement measures will nearly always be considered illegal.").

[79] *See* FED. R. CRIM. P. 41(b) (listing the sole instances in which our-of-district search warrants are permitted). *See also* United States v. Bin Laden, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000) (noting that "there is presently no statutory basis for the issuance of a warrant to conduct searches abroad").

officers.[80] All three exceptions extend to locations where the U.S. already exerts significant, if not exclusive, regulatory authority—thus avoiding potential conflict with foreign jurisdictions and maintaining respect for the exclusive, sovereign authority to enforce the law. Notably, the Supreme Court in 1990 considered and rejected a proposed amendment to the rule that would have permitted judges to issue extraterritorial search warrants in certain instances.[81]

These territorial-based limitations have recently come to the fore in the context of a pending Department of Justice (DOJ) proposed amendment to Rule 41.[82] The amendment would authorize the issuance of remote access search warrants for electronically stored data in situations where the location of the device or stored data being investigated is unknown. DOJ argues that this amendment is needed to address situations in which anonymization tools disguise the location of a computer or other device being used for criminal activity.[83] Although the government had previously argued that magistrate judges already had jurisdiction to issue such warrants under the existing version of Rule 41 on the grounds that the agents accessing the data would be within the magistrate's district, at least one judge rejected the government's request.[84] In the magistrate's words, the government's position would effectively "permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district"[85]—an argument with obvious parallels to the Supreme Court's concern in *Riley v. California* about agents accessing data stored in the cloud, far removed from the locus of the physical search.[86] The magistrate thus defined the relevant locus of the search and seizure as that of the computer or data being gathered, rather

---

[80] *See* FED. R. CRIM. P 4(b)(5).

[81] *See* FED. R. CRIM. P. 41, Notes of Advisory Committee on Rules – 1990 Amendment.

[82] *See* Advisory Committee on Criminal Rules, Proposed Amendment to Rule 41, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2014-04.pdf, at 165. The public has until Feb. 17, 2015 to submit comments on the proposed. The amendment will become effective on December 1, 2016 if approved by the relevant Advisory Committee, the Committee on Rules of Practice and Procedure, the Judicial Conference, and the Supreme Court, and Congress does not act to defer, modify, or reject it.

[83] *See* Raman Letter, *supra* note 8, at 2 (emphasizing that the circumstances "where investigators can identify the target computer, but not the district in which it is located – is occurring with greater frequency in recent years").

[84] *See* Sara Beale & Nancy King, Memo to: Members, Criminal Rules Advisory Committee, Re: Rule 41 proposal (Mar. 17, 2014), at 2, *available at* http://cryptome.org/2014/08/fbi-nit-tor-hack.pdf (page 156); Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance* (Dec. 6, 2013), http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html (describing use of remote search tools in a terrorism case).

[85] *In re* Warrant To Search A Target Computer at Premises Unknown, 958 F.Supp. 2d 753, 757 (S.D. Tex. 2013).

[86] 134 S. Ct. 2473, 2492 (2014).

than the location of the agents accessing the device. Since the location of the computer was unknown, there was no jurisdiction to issue the warrant.[87]

DOJ responded with its proposed rule revision. Its proposal creates the possibility (or more accurately, probability) that magistrates will be authorizing searches or seizures of data located extraterritorial. If the location of the target device and/or data is unknown, agents and reviewing judges will not know whether the device and associated data is located territorially or extraterritorially. In fact, data on Tor, one of the largest anonymity networks, indicates that 85 percent of its users connect to the network from *outside* the United States, meaning that extraterritorial searches are not only possible, they are likely.[88] Moreover, even when the targeted device is located territorially, the data accessed from the device may be stored extraterritorially.

In a letter to the Rules Committee, the Criminal Division's Acting Assistant Attorney General (AAG) responds to this possibility: "[S]hould the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but would . . . support the reasonableness of the search."[89] But this raises a series of as-of-yet unanswered questions about what agents will be instructed to do if and when they discover that they are engaged in an extraterritorial search: Will agents be obliged to cease the investigation as they seek the consent of the nation where the computer or data is located? Or can they continue their activities as they await the foreign nation's response? In fact, at least one magistrate has warned that he still might not be able to issue a warrant even with the rule change, given the risk of issuing an extraterritorial warrant.[90]

The government's position is notable for three additional reasons. First, DOJ appears to accept, contrary to its position in the earlier search warrant applications, that the relevant search or seizure occurs where the data is located, and not where the government accesses it. The letter explicitly asserts, "[i]n light of the presumption against extraterritorial application, this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries."[91] In other words, it assesses territoriality based on the location of the data, not the agents accessing data. Second, the government concedes that courts lack jurisdiction to issue Rule 41 search warrants for extraterritorially stored data. Third, the proposed amendment

---

[87] 958 F. Supp. 2d at 757 ("Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1).").

[88] *See* TOR Metrics: Users, https://metrics.torproject.org/users.html (last accessed Feb. 4, 2015; Ahmed Ghappour, *Justice Department Proposal Would Greatly Expand FBI Extraterritorial Surveillance*, Just Security, Sep. 14, 2014, at http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/ (raising concerns about the ways in which this amendment will lead to extraterritorial searches and seizures).

[89] Raman Letter, *supra* note 8, at 5.

[90] Conversation with Magistrate Judge Stephen Smith (June 5, 2015).

[91] *Id.* at 4.

covers not just devices held in unknown locations, but also stored data held in unknown locations. Such a warrant could, for example, be used to remotely access a computer and then use that computer to access data stored in the cloud. This could include data stored in whole, or in part, in Dublin, Ireland, or any of the many other data storage centers located extraterritorially.[92] Yet, according to the government's submission, if the government *knew* the data was being held in Ireland (as it does in the Microsoft case), the magistrate could *not* issue the warrant. Agents would be required to go through either the steps dictated by the Mutual Legal Assistance Treaty (MLAT) or an analogous process, just as Microsoft is arguing should be the case when the government, instead of accessing the data directly, compels an electronic communications provider to do so. The government's position with respect to the proposed amendment thus appears to depend on the fact that it is asking Microsoft to do the collection; it could not, according to its statements with respect to the Rule 41 discussion, unilaterally access the data itself.

(ii) Wiretap Authority

Adopted in part as a response to the Supreme Court's rejection of New York's eavesdropping statute, the Wiretap Act covers real-time interception of wire, oral, or electronic communications.[93] Every court to consider the issue has concluded that the Wiretap Act governs interceptions that occur within the territory of the United States only—a conclusion that is supported by the presumption against the extraterritorial application of statutes, the legislative history of the Act, and the territorial limits found in Rule 41 on magistrate's warrant jurisdiction.[94] That said, all of these cases have dealt with instances in which both the agents accessing the data and

[92] *See* Riley v. California, 134 S. Ct. at 2491 (2014) (noting that a cell phone can be "used to access data located elsewhere, at the tap of a screen").

[93] 18 U.S.C. § 2510 *et seq*. Among other criteria, the reviewing judge must make probable cause findings with respect to the targeted individual, targeted communications, and the facilities or place from which the communications are to be intercepted. *Id.* § 2518(3). Interception is subject to minimization requirements—requiring agents to take steps to avoid the acquisition of nonrelevant content—and strict limits on use and disclosure to others. *Id.* §§ 2517; 2518(5). *See also* Berger v. New York, 388 U.S. 41, 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.")

[94] *See e.g.,* United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987) (rejecting argument that wiretapping of telephones in Thailand could violate Wiretap Act); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978) (holding that Wiretap Act did not apply to extraterritorial interception in Canada); United States v. Toscanino, 500 F.2d 267, 279-80 (2d Cir. 1974) ("[T]he statute significantly makes no provision for obtaining authorization for a wiretap in a foreign country."); United States v. Angulo-Hurtado, 165 F. Supp. 2d 1363, 1369 (N.D. Ga. 2001); *see also* S. Rep. No. 99-541, at 12 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (emphasizing that the Electronic Privacy Act, which amended the Wiretap Act, "regulates only those interceptions conducted within the territorial United States").

data being accessed were outside the United States.[95] The court has not yet addressed a situation in an interception order is issued for a device that is located or travels outside the United States, but is being listened to by agents located within the United States.

The analogous issue has, however, come up with respect to court jurisdiction over wiretap orders for interceptions that take place *within* the United States. In contrast to Rule 41 cases, which seem to assume that the location of property is what controls, several Wiretap Act cases have suggested that—consistent with the government's position in the Microsoft case—territoriality be assessed based on *either* the location of the agent accessing the data or the location of the data. In interpreting the jurisdictional provision of the act—permitting judges to authorize the "interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting"[96]—numerous district and circuit court cases have looked to both the locus of the device being tracked *and* the locus of the agents conducting the intercept and listening to the data as a basis for establishing territoriality.[97] In other words, so long as *either* the agents listening in on the conversations or the device or wires being listened to is within the judge's district, then jurisdiction (i.e. territoriality) is met.

But the issue is not settled. At least one Circuit Court has disagreed, concluding that a physical listening device must be installed within the authorizing court's district, even if agents will be monitoring from within the district. [98] Moreover, these cases have all involved a situation in which when both the agents and device being monitored were located within the United States, leaving unresolved the applicable rule either the device being monitored or the agents doing the monitoring were located extraterritorially.

(iii) The Stored Communications Act

A separate statutory scheme governs the collection of stored communication—the statute at the heart of the Microsoft dispute. Passed

---

[95] In United States v. Cotrini, 527 F.2d 708 (2d Cir. 1975), the Second Circuit considered and rejected, the argument that there was a sufficient territorial nexus to trigger the application of the Wiretap Act simply because the intercepted telephone conversations had *traveled* over the nation's communication system. *See also* Zheng v. Yahoo! Inc., 2009 WL 4430297 (N.D. Cal. Dec. 2, 2009).

[96] 18 U.S.C. § 2518(3).

[97] *See, e.g,* United States v. Luong, 471 F.3d 1107, 1109 (9th Cir.2006) ("[T]he most reasonable interpretation of the statutory definition of interception is that an interception occurs where the tapped phone is located *and* where law enforcement officers first overhear the call."); United States v. Ramirez*,* 112 F.3d 849, 852–53 (7th Cir.1997) (same) ;United States v. Denman, 100 F.3d 399, 403 (5th Cir.1996) (same); United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir.), *cert. denied,* 506 U.S. 847, 113 S.Ct. 140, 121 L.Ed.2d 92 (1992) (same).

[98] United States v. Glover, 736 F. 3d 509, 514-15 (finding Title III warrant invalid because the mobile interception device was installed on property located outside the authorizing judge's jurisdiction)

in 1986, as part of the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA) criminalizes unauthorized access to and disclosure of stored communications, and lays out the procedures and standards by which law enforcement agents can lawfully compel disclosure from ISPs.[99] It specifies different forms of compulsory process—subpoena, court order, and warrant—that vary in terms of requirements and application.[100] By the terms of the statute, a subpoena can be used to obtain a range of non-content information from service providers, including their customers' names, addresses, payment information, and records of session times and duration.[101] When proceeding by subpoena, the government must either notify the customer, thus providing an opportunity to object, or obtain a delayed notification order.[102] A court order is required to obtain the historical logs detailing the email addresses with which the customer has communicated, based on a finding of "specific and articulable facts" that the information sought is "relevant" to an ongoing criminal investigation.[103] By statute, a warrant based on a finding of probable cause is required to compel an electronic service provider to disclose content of communications (*i.e.,* emails) stored for 180 days or less.[104] Several courts have concluded that, as a matter of constitutional law, the warrant requirement also applies to emails stored more than 180 days and remotely stored emails not otherwise covered by the statutory warrant requirement.[105]

---

[99] For a thorough analysis of the Stored Communications Act, *see* Orin Kerr *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 GEO. WASH. L. REV. 1208 (2004). *See also* Kerr, *The Next Generation*, *supra* note 10.

[99] *See* 18 U.S.C. § 2703 (2008).

[100] *Id.*

[101] *Id;* § 2703(c)(2).

[102] *Id.* §§ 2703(b); 2705 (2008) (describing delayed notification standards and procedures); *id.* § 2705(2)(defining "adverse result" as "endangering the life of physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial")(numbering omitted).

[103] 18 USC § 2703)(c)(1); id. § 2703(d).

[104] *Id.* § 2703(a). At the time, this was understood as covering the vast majority of stored emails; limited storage capacity meant that only a small fraction of emails would be stored past 180 days. This is no longer the case. *See* Kerr, *The Next Generation*, *supra* note 10. For a critique of the Stored Communications Act as insufficiently protective of privacy interests, *see* David J. Solove, *Reconstructing Electronic Surveillance Law,* 72 GEO. WASH. L. REV. 1264, 1298 (2004).

[105] *See* is United States v. Warshak, 631 F.3d 266, 288 (6th Cir, 2010) ("[T]o the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly, [that portion of] the SCA is unconstitutional."); *In re* Applications for Search Warrants for Info. Associated with Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012); United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012); State v. Hinton, 280 P.3d 476, 483 (Wash. Ct. App. 2012); *see also* Theofel v. Farey-Jones, 359 F. 3d 1066, 1075-77 (9th Cir. 2003) (rejecting government's argument that a warrant is not required to access a backup copy of a customer's opened email that is held on the providers server) That said, the government continues to argue that *Warshak* got it wrong, that the Fourth Amendment does not apply to email held by a third-party provider, and that in any event there is no search or seizure until the emails are

The legislative history, coupled with the presumption against extraterritoriality, overwhelmingly supports the conclusion that the SCA's warrant provision does not apply extraterritorially. (In fact, this is one of the few areas of agreement between the government and Microsoft in its ongoing litigation; they disagree, however, about what this means.) The 1986 House Judiciary Committee Report on the SCA states that the "provisions regarding access to stored wire and electronic communications are intended to apply only to access in the territorial United States."[106] When Congress amended the statute in 2001 to authorize magistrates to issue multi-district warrants, the amendment was entitled "*Nationwide* Service of Search Warrants for Electronic Evidence."[107] It is thus not surprising that the one case to squarely presented the question of the statute's geographic reach to date concluded that it was territorially limited. In *Zheng v. Yahoo!*, a district court judge rejected the plaintiff's argument that the SCA applied to the conduct of Yahoo! China.[108] The case, however, was relatively straightforward: the data was located in China; the Yahoo! China employees who accessed the data were in China; and the disclosures took place in China.[109] The key question therefore was whether Yahoo! (based in the United States) exercised sufficient control over Yahoo! China to bring its actions within the jurisdiction of the United States. The district court concluded that it did not.

Thus, as with the Wiretap Act, it is clear that a territorial presumption applies, but the question of *how* it applies when the data and the person or entity accessing the data are separated by an international border remains unsettled. What is the relevant location for determining territoriality—that of the Internet Service Provider accessing the data, or that of the data itself?

In answering this question in the Microsoft case, the government argues that it the location of the ISP that controls. In making that claim, the government focuses on language of the Act, which authorizes the use of a warrant to "require disclosure," operates as a form of compulsory process, much like a subpoena.[110] It then draws on rules governing subpoenas, which require the recipient of the subpoena to turn over information within its control, irrespective of its location, to argue that the location of the ISP is what matters.

But as Microsoft and several amici note, however, there are two key flaws with this argument: First, Congress used the term "warrant," not subpoena; there is thus good reason to think that the rules governing

---

actually opened and reviewed by government agencies. *See* Oral Argument Tr., *supra* note 1, at 4.

[106] H.R. REP. NO. 99-647, at 32 (1986).

[107] Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56 § 220, 115 Stat. 272, 291-92 (2001); H.R. REP. NO. 107- 236, at 57 (2001).

[108] Zheng v. Yahoo! Inc., No. C-08-1068 MMC, 2009 WL 4430297, *4 (N.D. Cal. Dec. 2, 2009).

[109] *Id.* at *1, 4.

[110] *See* Appellee Brief, Microsoft, *supra* note 1, at 17.

warrants, not subpoenas, control. Second, even if the analogy to subpoenas is the correct one, subpoenas have long been relied on to compel disclosure of a company's *own records*; they have not been relied on to compel disclosure of a *customer's* private data that has been stored with the company. The government could not, for example, rely on a subpoena to compel a post office to turn over mail it is transporting, a bank to turn over the contents of a customer's safety deposit box, or a landlord to collect and turn over the papers stored in a tenant's home. This is for good reason. One does not (and should not) lose a reasonable expectation of privacy in property—as arguably distinct from the metadata that the company needs to transmit a message from place to place or identify the proper user—that is being entrusted with a third party for the limited purposes of transmittal or storage.

Moreover, while the government points out the many costs of making location determinant of the rules that apply, including the possibility of nefarious actors moving key evidence outside the jurisdiction of the United States, there are at least four countervailing policy reasons to be concerned about a rule that permits the government to compel an ISP to turn over customer emails or stored documents, without regard to location. First, at least absent the development of new norms with respect to the collection of data, such a rule runs counter to the long-standing international law prohibition against unilateral law enforcement action within another sovereign's territory, and thereby creates international friction and perhaps even a direct conflict of laws.[111] Second, and relatedly, it puts ISPs in the difficult position of being potentially subject to two competing sets of rules and regulations—that of the requesting state and that of the state where the data is stored. Third, it fuels data localization movements and encourages those located outside the United States to seek out alternatives to U.S.-based providers, with significant costs to U.S. businesses and the development of the global Internet as a whole.[112] Fourth, and perhaps most importantly, it makes it hard for the United States to object when other nations compel U.S.-based ISPs to turn over data stored in the United States, in contravention of U.S. law and privacy protections. This is not an idle concern. Already, the UK has passed legislation that permits its government to compel stored communications from any ISP that does business within the UK's jurisdiction, regardless of

[111] *See, e.g.,* Brief of Amicus Curiae Ireland at 3, *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft, no. 14-2985-CV (2d Cir. Dec. 23, 2014) ("Ireland respectfully asserts that foreign courts are obliged to respect Irish sovereignty (and that of all other sovereign states) whether or not Ireland is a party or intervener in the proceedings before them.")

[112] *See, e.g.,* Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders*, THE HAGUE INSTITUTE FOR GLOBAL JUSTICE (May 1, 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275.

where the data is stored, if the request is based on specified law enforcement or national security reasons.[113]

I return to these issues in Part III. For now, it is simply worth noting that while ECPA is rightly understood to have territorial reach, the question of what is territorial and what is extraterritorial is in sharp dispute. And neither the text nor legislative history provides the necessary guidance. The issue was not on the minds of the drafters of ECPA, which was written at a time when the Internet was still in its infancy and few communications crossed international borders.[114] And none of the subsequent amendments to ECPA address the statute's extraterritorial reach or the key question presented in the Microsoft case—whether directing a U.S.-based service provider to disclose data located outside the United States is a territorial or extraterritorial action?

* * *

To sum up, territoriality is a critical factor in assessing both the reach of the Fourth Amendment and the scope of the government's authority to search and seize. In fact, it is often determinant of the rules that apply. That said, territoriality serves different underlying purposes in the different areas in which it operates. Territoriality in the context of the Fourth Amendment serves as a proxy for the notion that only "the people" are entitled to the Fourth Amendment's protections—a category that excludes most non-U.S. citizens located abroad. The Fourth Amendment thus binds the government when it searches or seizes property within the United States, but poses no constraint when the government is searching or seizing the property of an alien lacking substantial connections to the nation that is located outside the United States.

The nation's foreign intelligence surveillance scheme adopts this basic approach, with the targeting of U.S. persons and persons located within the United States subject to heightened procedural and substantive protections as compared of non-U.S. persons located outside the U.S. boundaries; and collection of data physically located in the United States subject to heightened regulation and oversight as compared to collection of data located outside the United States. As with the Fourth Amendment, the underlying assumption is that U.S. citizens and legal permanent residents deserve enhanced privacy protections.

Territoriality in the context of warrant jurisdiction is equally important, but serves a very different purpose. It stems from respect for other states' sovereignty, as well as an appreciation of the political and diplomatic consequences of failing to do so. Under international law, the

[113] Data Retention and Investigatory Powers Act, 2014, c. 27 (U.K.) §4(4) (amending the Regulation of Investigatory Powers Act 2000 (U.K.) §11. *See also* House of Commons, Data Retention and Investigatory Powers Bill, Explanatory Notes (14 July 2014) § 15, http://www.publications.parliament.uk/pa/bills/cbill/2014-2015/0073/en/15073en.pdf.

[114] *See* Kerr, *The Next Generation, supra* note 10, at 405 ("[T]he possibility that individuals outside the United States might use U.S.-based services—or that individuals inside the United States might used services based abroad—never arose.").

unilateral exercise of law enforcement in another state's territory is deemed a breach of that state's sovereignty, potentially justifying counter-measures. While there may be times when law enforcement or national security interests justify such a breach of international law, this is generally a decision that is made by the political branches after a full analysis of the costs and benefits--not a decision delegated to the 500-some magistrate judges and hundreds of state court judges scattered across the country.[115] Territorial limits on warrant jurisdiction reflect this basic understanding.

But, as the following section highlights, data is beginning to challenge these long-standing assumptions.

II. DATA IS DIFFERENT

Territorial-based distinctions—whatever their purpose—depend, at their core, on the ability to distinguish between the relevant "here" and "there," and a determination that the "here" and "there" matter. Data, and the manner in which it is accessed and controlled, is undercutting both of these foundational assumptions. The disconnect between the user and his or her data, as well as the disconnect between the government agent accessing the data and the physical location of the data itself, is beginning to raise questions about what is territorial and what is extraterritorial. Meanwhile, the mobility, divisibility, and intermingling of data is beginning to raise questions about the normative significance of data's location at any given moment. This section explores how data differs from its tangible counterparts and why these differences matter—focusing in particular on data's mobility, divisibility, location independence, intermingling and third party control.[116]

A. DATA'S MOBILITY

When physical objects move from place to place, they are constrained by the ordinary laws of physics, as well as generally observable and conscious choices about how to move from A to B. A person traveling from Washington, D.C. to Philadelphia will generally take the most direct route, crossing through Maryland and Delaware on the way. If the traveler detours to France, it is likely the result of a planned decision. The same is

[115] *See* 18 U.S.C. § 2703(c)(1)(A) (2009) (authorizing federal magistrates, federal judges, and state court judges to issue ECPA warrants, pursuant to the requisite procedures); Federal Magistrate Judges Association, http://www.fmja.org/about-us.html (last accessed Nov. 4, 2014) (stating that there were 527 full-time magistrate judges in 2011).

[116] Not all of this is new. The international community has, for some time, for example, been dealing with the rapid flow of money across borders and the complicated jurisdictional issues that this poses for a combination of regulatory, taxation, and enforcement purposes. Some of these observations thus have relevance to these other areas of law as well; and some of the regulatory and enforcement mechanisms designed to deal with things like cross-border flows of money provide possible models for thinking through some of the challenges posed by law enforcement demand for data across jurisdictional boundaries. This is an area I intend to explore further in future work.

true for data's closest tangible counterpart—mail. It is highly unlikely that either USPS or UPS would send a letter through Paris on the way from Washington, DC, to Philadelphia, absent some significant snafu. Similarly, when one stores tangible property in a safety deposit box or locked storage unit, it has a known, observable, and fixed location. Absent a theft or seizure of property, it will stay there until the owner decides to move it elsewhere.

Data's mobility—in particular its speed and unpredictability—challenges our understanding of both what it means to transit from place to place and what it means to "store" our property.[117] When two Americans located in the United States send an email, the underlying 0s and 1s generally transit domestic cables. But they also, with some non-negligible frequency, exit our borders before returning and showing up on the recipient's computer screen.[118] When one Google chats with a friend in Philadelphia or uses FaceTime with a spouse on a business trip in California, the data may travel through France, without the parties to the communication knowing that this is the case. Similarly, when data is stored in the cloud, it does not reside in a single fixed, observable location akin to a safety deposit box. It may be moved around for technical processing or server maintenance reasons, and it may be copied, possibly divided up into component parts and stored in multiple places, some territorial and some extraterritorial.[119] At any given moment, the user may have no idea—and no

[117] In making this claim, I assume that the author of a document or unsent email retains a reasonable expectation of privacy in the data, even if it is stored by a third party provider.

[118] *See, e.g.,* Statement of General Michael V. Hayden, Director of the Central Intelligence Agency, Modernization of the Foreign Intelligence Surveillance Act, Before the S. Judiciary Comm., 109th Cong. (2006), www.judiciary.senate.gov/imo/media/doc/hayden_testimony_07_26_06.pdf ("A single communication can transit the world even if the communicants are only a few miles apart."); Marshall Brain & Tim Crosby, *How Email Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/e-mail-messaging/email.htm (last visited Nov. 10, 2014) (describing the path taken by an email through servers before reaching its final destination).

[119] *See, e.g.*, Oral Argument Tr. *supra* note 1, at 48 ("Data can be stored at any place, at any time. . . . [T]oday with cloud services, it has become increasingly common for the location of data to change from day to day, or hour to hour. You can have the contents of a single account distributed across multiple servers."). *See also* John M. Cauthen, *Executing Search Warrants in the Cloud*, The FEDERAL BUREAU OF INVESTIGATION (Oct. 7, 2014), www.leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud ("[I]n a cloud-computing environment . . . little, if any, data pertaining to a computer user is found in a single geographic location."); GOOGLE, http://www.google.com/about/datacenters/inside/data-security/index.html (last visited Nov. 10, 2014) (detailing Google's data storage across multiple servers in various locations to chunk and replicate data). *But see* Brief for Computer and Data Science Experts as Amicus Curiae Supporting Appellant at 21, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (No. 13 Mag. 2814) ("[I]mpracticalities of . . . partitioning very small segments of data across geographically dispersed data centers mean that a given individual's email will generally be isolated to a particular region, if not a particular datacenter and server, regardless of the vendor.").

ability to know—where his or her data is being stored, moved to, or the path by which it is transiting.

These distinctions between tangible property and data matter for at least two reasons. First, they highlight the potential arbitrariness of data location as determinative of the rules that apply. Whereas the location of one's own person and tangible property is subject to generally understood rules and limitations on the way physical property moves through space, data can move from point A to point B in what appears to be circuitous and arbitrary ways, all at breakneck speed based on computer algorithms, rather than specific human choice. This is precisely the government's point in the Microsoft case when it warns against the "arbitrary outcomes" that would result if government access to data depended on where a provider chooses to hold data at any given point in time..[120] And while the government fails to make the point, the same argument can be made with respect to privacy protections that turn on data location.

Second, the path of travel is often done without the knowledge, choice, or even input of the data user.[121] This matters for purposes of both notice and consent. It is widely understood that when one travels to or retains property in a foreign jurisdiction, one is subject to the sovereign nation's rules and regulations. Individuals and entities are required to conform their behavior accordingly or accept the consequences. But if an individual sends an email to a friend in Philadelphia that happens to transit through another nation, that person is not consciously choosing to bind himself to any particular foreign government's laws. Nor is the user consciously choosing to relinquish protections guaranteed by laws governing search and seizure of property in the United States simply because the data happens to transit outside the United States. Similarly, when one stores data in the cloud, one often has little control or even knowledge about the places where it is being held (decisions that are instead entrusted to computer algorithms)—and thus what presumptions and rules apply.

B. DATA'S DIVISIBILITY AND DATA PARTITIONING

[120] Appellee Brief, Microsoft at 53. Microsoft counters that the location decisions are hardly arbitrary, but instead designed to keep data physically near the user to the maximum extent possible, so as to minimize network latency—the delay between the time the data is requested and the time it is delivered. *See In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*,* 15 F. Supp. 3d 466, 467 (citing Microsoft affidavits) ("[B]ecause the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter."); *see also* Brief for Computer and Data Science Experts as Amicus Curiae Supporting Appellant at 20, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (No. 13 Mag. 2814) (noting that Google seeks to keep data near its Gmail users).

[121] *See, e.g.*, Cauthen, *supra* note 111 ("The problem is that finding where . . . data is physically stored can be very difficult—even the user might not know where it is.").

Data stored in the cloud is often copied and held in more than one location, thereby protecting against server malfunctions and ensuring that a user can continue to access his or her data from a backup location. Some storage locations might be territorial and some might be extraterritorial.[122] This is akin to making multiple copies of one's documents and storing them in multiple jurisdictions, and is not, by itself, unique to data. But the ease and speed by which data can be copied and moved has led to an exponential increase in multi-site, and often multi-nation, storage—raising questions about whether it is even possible to identify and isolate a specific data location.

Data partitioning, under which a single database is divided into multiple parts so as to increase the manageability and efficiency of use, adds another layer of complication.[123] The various components of a partitioned database may be held in multiple locations. And in certain instances, so-called "relational databases" are only comprehensible if pulled up using the appropriate application.[124]

Data divisibility and data partitioning thus highlights the potential arbitrariness and complications of making data location determinative of the rules that apply. Can the government evade Fourth Amendment protections that apply to a non-U.S. person's data stored within the United States by locating a back-up copy stored extraterritorially? Can and should the United States demand that U.S.-based ISPs retain copies of their customer's data within the territorial jurisdiction of the United States, so as to avoid the kinds of foreign policy concerns being addressed in the Microsoft case? In a relational database, is the relevant location the place from the data is accessed and reassembled in a usable form, or the location where each of the component parts are stored? Under analogous rule for tangible property, the location of each component part would control. But this would require a territoriality determination—and possibly the application of different rules—for the acquisition of the various parts of a sought-after account or database. As these questions suggest, data location is both highly manipulable and in some cases difficult to define, raising important questions about both its normative significance and its ability to provide a stable determinant of the applicable rules.

---

[122] *Data Center Locations*, GOGGLE.COM, http://www.google.com/about/datacenters/inside/locations/ (last visited Feb. 13, 2014); Sasha Segall, Note, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1114-15 (2013).

[123] *See, e.g*, Ian Walden, *Accessing Data in the Cloud: The Long Arm of t Law Enforcement Agent*, QUEEN MARY UNIVERSITY OF LONDON, SCHOOL OF LAW (Nov. 14 2011), *available at* http://ssrn.com/abstract=1781067 ("Techniques widely used in cloud computing, such as 'sharding' or 'partitioning,' mean that the data will likely be stored as fragments across a range of machines, logically linked and reassembled on demand, rather than as a contiguous data set."); Tony Morales, *Oracle Database VLDB and Partitioning Guide,* ORACLE, 1-2 (July 2007), http://docs.oracle.com/cd/B28359 _01/server.111/b32024/title.html (describing the benefits of partitioning).

[124] *See* Cauthen, *supra* note 111.

C. LOCATION INDEPENDENCE

i. Disconnect Between Location of Access and Location of Data

One of the biggest changes wrought by modern technology is the possible disconnect between the location of the government actor doing the searching or seizing and the location of the property or person being seized. Whereas the search of tangible property or seizure of a person generally involves the co-location of the government agents and target of the search or seizure, the rise of modern technology means that this is no longer always the case.[125] This is certainly the case with respect to data—but it is also true in other areas as well, thanks to technological developments. The following analyzes how courts and the executive have addressed this disconnect in the context of guns and drones, and then explores how the additionally unique features of data change the analysis.

In *Hernandez v. United States*, a U.S. border patrol agent was standing in Texas when he shot the decedent just over the border with Mexico, thus creating a disconnect between the location of the government actor (territorial) and the location of the target (extraterritorial). Although the en banc Fifth Circuit issued a highly fractured opinion as to the reach of the applicable constitutional rights, all fifteen judges simply assumed, without analysis, that the relevant location was that of the target, and that the seizure was therefore extraterritorial.[126] The use of drones provides an even more extreme example: drone operators sitting in Langley, Virginia, or at any one of a number of military bases, can remotely pilot a drone and drop a bomb half-way around the world in, say, Yemen, Somalia, or Iraq. Yet virtually every legal and policy analysis of drone strikes assumes that such targeted killings constitute extraterritorial actions (i.*e.*, seizures), regardless of the location of the drone operator.[127]

By straightforward analogy to guns and drones, the search and seizure of data would be understood to take place where it was stored and manipulated, rather than (or in addition to) where it was accessed or reviewed. And that is how courts and the government have generally considered the issue of search and seizure of data on personal computers—focusing on the location of the computer where the data is stored, rather than the location of the government actor. In *United States v. Goshkov*, for example, agents located in Seattle remotely accessed and copied data from a computer in Russia. The district court deemed this an extraterritorial search because the computer was located overseas at the time it was accessed—making the location of the data, rather than the agents, the key determinant

---

[125] *See, e.g.* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (noting that, thanks to cloud computing, "[c]ell phone users often may not know whether particular information is stored on the device or [on remote servers] in the cloud, and it generally makes little difference.").

[126] Hernandez v. United States, 11-50792 (5th Cir. Apr. 24, 2015) (en banc).

[127] *See, e.g.*, OLC Al-Aulaqi Memo, *supra* note 6.

of territoriality.[128] (Russia deemed this an extraterritorial search as well, asserted it was a violation of its domestic law and filed criminal charges against one of the FBI agents involved.[129]) In commenting on the proposed change to Rule 41 to permit the issuance of remote search warrants (discussed in Part I(C)(i)), the government similarly seemed to accept that the territoriality analysis depended on where the data was located—not on the location of the government agent remotely accessing or manipulating the data.[130]

But, as the government's position in the Microsoft case suggests, this seemingly straightforward application of rules applicable to drones and guns to the world of data is not the only possibility for thinking about the locus of the relevant search or seizure of data. There is, after all, a key difference between shooting a gun or activating a remotely controlled drone, on the one hand, and the manipulation of the type of data at issue in the *Gorshkov* or Microsoft case, on the other. When a government agent shoots a gun across the border or launches a drone in Somalia, there is an apparent, tangible invasion of airspace, as well as an apparent, tangible effect in another nation's territory—an explosion and possible killing of individuals or destruction of property. But when the government or its agents in State A remotely access a server in State B and copy data located there, there is often no observable effect in State B, nor any change in the data user's ability to access and use the data.[131]

In fact, the absence of any alteration or interference with the user's ability to access his or her data has led some to suggest that the copying of the data does not even amount to a constitutionally relevant seizure, thereby making the Fourth Amendment framework irrelevant. Orin Kerr, for example, initially asserted that copying of data is not a search and seizure for Fourth Amendment purposes because it leaves the data owner's possessory interests intact.[132] The magistrate judge in the Microsoft case agreed, and cited to Kerr for the proposition that the relevant constitutional moment first occurs when the data is reviewed in the United States—not when it was merely copied.[133] But Kerr later changed his perspective, concluding that

---

[128] United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (D. Wash. May 23, 2001) ("[A]gents' extraterritorial access to computers in Russia and their copying of data thereon" as not covered by the Fourth Amendment since it was an extraterritorial action directed at a non-citizen located outside the United States.).

[129] Mike Brunker, *FBI Agent Charged with Hacking*, MSNBC (Aug. 15, 2002), http://www.nbcnews.com/id/3078784/#.VM178lph3L9.

[130] *See supra*, Part I(C)(i)

[131] *But see, e.g.,* Walden, *supra* note 115, at 4 (noting that remote data retrieval may yield data changes, particularly when accessed through certain types of cloud-based interfaces or unknown architecture).

[132] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 557-62 (2005).

[133] *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft*,* 15 F. Supp. 3d at 472. The Fourth Amendment argument is a bit of a red herring, as it is largely irrelevant to the central question about warrant jurisdiction under ECPA and the related questions of international comity. State A can still interfere with State B's sovereignty even if the action does not rise to the level of a search or seizure

copying of Fourth Amendment protected data for information-gathering purposes *is* a constitutionally recognized seizure.[134] As Kerr ultimately concludes, the Fourth Amendment's prohibition on unreasonable seizures is designed to protect against, among other things, the indiscriminate collection of information not already available to the government; when the copying of adds to the pool of available information to the government and deprives the user of the right to exclude, it constitutes a Fourth Amendment seizure.[135] Kerr's latter argument, although arguably at odds with Supreme Court precedent,[136] seems the better one, as evidenced by the numerous other scholars and courts that have similarly concluded that the copying of electronic data constitutes a seizure.[137]

But the mere fact that this is even an active debate highlights the ways in which data is different. Unlike an explosion from a gun or missile, the extraterritorial copying of 0's and 1's can be done surreptitiously and without any observable change to conditions in State B. This thus opens up the space for the government's argument not yet made with respect to guns and drones—that the location of access, not the location of the data, is what counts.

ii. Disconnect between Data and the Data User

Location independence between data and the data user is central to the efficiency of the cloud, and refers to the idea that data need not be stored in the same location as, or anywhere near, its user. This allows users

---

under Fourth Amendment doctrine. An FBI agent who went through a suspect's garbage in Dublin, without the knowledge and consent of the Irish government, would almost certainly be violating prohibition on unilateral law enforcement activities in another state's territory, even though looking through garbage is not a search under current Fourth Amendment doctrine. *See* California v. Greenwood, 486 U.S. 35 (1988) (concluding that collection and rummaging through garbage is not a search).

[134] Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L. J. 700, 704 (2010).

[135] *Id.* at 709-714.

[136] *See* U.S v. Jacobsen, 466 U.S. 109 (1984) (emphasizing that a seizure requires an interference with an individual's possessory interest in property). When data is merely copied and not removed or otherwise altered, the target's possessory interests are arguably unaffected. The claim, therefore, has to turn on some alternative possessory interests beyond the interest in using and manipulating the data; it also must include the possessory interest in excluding and determining who, and under what circumstances, is permitted to access the property.

[137] *See, e.g.,* Brief for Brennan Center for Justice at NYU School of Law et al. as Amicus Curiae Supporting Appellant at 4, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (No. 13 Mag. 2814) ("The Fourth Amendment "moment" occurs at the point the data is copied and produced to law enforcement, regardless of when or whether an officer might look at it."); Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39 (2002); Paul Ohm, *The Fourth Amendment Right to Delete,* 119 HARV. L. REV. FORUM 10 (2005); *cf.*, United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search.").

to access their data from wherever they are located, and it allows providers to move data in ways that minimize the use of storage centers at peak (high-cost) times, avoid down servers or power outages, and perform server maintenance without disruption of user access—and/or having to get the user's consent each time the data is moved around.[138] Meanwhile, the user is often blissfully ignorant of where his or her data is stored.

As discussed above, this raises normative questions about making data location determinant of the rules that apply. We generally assume that the location of one's tangible property is a product of choice and that it indicates a connection to the place in which the property is located. But with data, this basic assumption of a link between the interests of the person and the location of his or her property falls apart. When the user has no knowledge where his or data is at any given moment, it is hard to claim that data location means much to the user. This thus reinforces the point made earlier, that data location at any given point in time is neither a good indicator of the data user's ties to a particular location, nor fair determinant (from the perspective of the user) of the rules that ought to apply.

The location independence of data and its user also creates practical problems for law enforcement officials seeking to abide by the law. First, as the Supreme Court recognized in *Riley v. California*, even when agents locate a target's smart phone, computer, or other electronic device, they often will not know where the data that can be accessed on the device is physically being held.[139] This creates hurdles for law enforcement. Even when the government has a device and all the necessary passwords in its possession, it will not necessarily be able to ascertain—thanks to the cloud—whether it is accessing data that is stored territorially or extraterritorially.[140] (This problem, of course, does not arise when the government is, as in the Microsoft case, compelling the data directly from the third party provider that holds the data and can ascertain its location.)

Second, location independence of data and the data user means that, even when law enforcement officers can determine the location of data, they may not know anything about the location of the data user, let alone the degree of his or her connections to the United States. Imagine, hypothetically, a law enforcement agent trying to track down the location—and identity—of the source of an email describing plans to remotely detonate explosives on an upcoming parade. The agent needs to connect the data to a particular device; determine the location of the device; and then ascertain the location of the user of the device, which, absent real-time tracking, may not be the same as the device itself. Finally, the agent may

---

[138] Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313, 325-28 (2013) (outlining the basic structure and efficiencies of cloud computing).

[139] 134 S. Ct. at 2491 (noting that "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or had been pulled from some other location in the cloud.")

[140] *See also supra,* Part I(C)(i) (discussing this problem in the context of remote search warrants).

need to determine the identity of the user—*i.e.,* whether or not the user is a citizen or non-citizen with substantial voluntary connections to the United States. While this might be feasible, albeit difficult, when dealing with discrete targets for law enforcement purposes, the sheer quantity of data collected under current surveillance programs makes it impossible to do on an individualized basis.[141] Instead, the intelligence communities rely on—as they must—certain presumptions, such as the presumption that a target of unknown location is a non-U.S. person.[142] While often good proxies, such presumptions will inevitably be over or under-inclusive in some non-negligible number of cases. Meanwhile, the use of anonymization tools compounds these identification difficulties for law enforcement and intelligence agents alike.

Such identification difficulties are not unique to data. After all, if FedEx does an inspection of a suspicious looking package, discovers cocaine, and turns that information over to the government, law enforcement agents will need to track down the sender of the package. Perhaps there is a clearly written return address that takes them directly to the sender, but, more likely, there is no return address, a false one, and/or the address is accurate but the sender is no longer located there. Even with tangible evidence, identification problems can confound. But the quantity of data, the rise of anonymization tools, and the circuitous way data transits from place to place, magnify and exacerbate the difficulties. These difficulties raise questions about the viability of schemes that depend on user location and identity as determinative of the rules that apply.

D. DATA'S INTERMINGLING

Data is also different from tangible analogs in the way it can and often does intermingle property of multiple users. As discussed in Part I(B), communications transiting the fiber-optic networks are often bundled together as multi-communication transactions. NSA currently lacks the technological capacity to separate out these communications into their discrete components. Thus, if any one of the multiple communications is "to," "from," or "about" a non-US person that is the target of the surveillance, it acquires the entire transaction. Discrete communications that are part of the transaction, but not "to," "from," or "about" the target—including transactions to or from U.S. persons—are thus acquired, even though they could not be independently collected had they been transiting the fiber optic lines on their own. This highlights the difficulty of effectively implementing any user and identity-based distinctions, at least at the stage at which data is collected.

The intermingling of data also raises questions about how to ascertain the relevant data user for purposes of making a territoriality

---

[141] *See, e.g.,* Banks, *supra* note 10, at 1645 (emphasizing the difficulty of ascertaining user location).

[142] *See supra*, notes 59-61 and accompanying text.

determination and thereby determining what rules apply. Consider, for example, a Google document, which is not yet accessible to the general public, but potentially accessible to multiple private users. Or a multi-person chat that involves multiple users all employing encryption and thus exhibiting an intention to keep the chat private. Even if one could ascertain the location and identity of each user who accesses the Google document, or the location and identity of all participants in the multi-person chat, whose location and identity should count?[143]

Congress considered this issue in relation to 702 collection, placing a special prohibition on the acquisition of what are described as "domestic communications." But, as described above, Congress defined domestic communications restrictively, to include only those communications in which the sender and *all* recipients are located in the United States.[144] This means that if one sends an email to multiple family members, one of whom happens to be temporarily overseas, the message is treated differently than if it had not included that single overseas recipient. This was a conscious choice on the part of Congress–done to increase the aperture of collection for purposes of gathering foreign intelligence information. But why should this be the rule: Why should restriction apply only when *all* the recipients are in the United States, as opposed to whenever *one* of the intended recipients is based in the United States? These and other related difficulties in ascertaining whose location and identity is determinative of the rules that apply further highlights the complexity of implementing the territorial and identity-based distinctions required by law.

E. THIRD PARTY ISSUES

Most tangible property is retained by the owner him or herself, with only a small portion turned over to third parties to manage or execute. By contrast, large quantities of digital property is held by or transits through, property controlled by third parties, including, for example, electronic service providers, cloud service providers, and the companies that maintain and operate the fiber-optic cables that make up the Internet backbone.[145] Moreover, it is these third parties, not the user, that often make critical decisions about the path by which data travels or where it is stored. It is also the third party, not the user, that is often called on by government officials to collect and produce sought-after data.

---

[143] *See also* Kerr, *The Global Internet, supra* note 12, at 317 (warning of the possibility of "conflicting standards when multiple individuals have Fourth Amendment rights in a communication").

[144] 50 USC § 1881a(b)(4)(2008).

[145] *See, e.g.,* Rich Miller, *How Dropbox Stores Stuff for 200 Million Users*, Data Center Knowledge (Oct. 23, 2013), http://www.datacenterknowledge.com/archives/2013/10/23/how-dropbox-stores-stuff-for-200-million-users/ (describing how Dropbox utilizes Amazon servers to maintain client data).

There is a rich and important literature about the so-called third party doctrine—the idea born from two 1970's Supreme Court opinions (*Smith v. Maryland*[146] and *United States v. Miller*[147]) that data exposed to third parties is not protected by a reasonable expectation of privacy. As many others have noted, the quantity and type of information at stake in the cases that spawned the doctrine—the telephone numbers dialed on a single day and four months' worth of bank records—was limited by the facts of the cases and technology of the time.[148] It is now no longer feasible to live in and participate in a digital world without exposing one's data, and hence one's most private thoughts and associations, to a third party. And there is good reason to think that the Supreme Court may soon conclude that the third party doctrine has been stretched beyond recognition and begin to set some limits.[149] That said, my point here is not to resolve the difficult questions raised by the third party doctrine, but simply to note that the third party issues create yet another point of divergence from most other forms of tangible property.

Such third party control matters for two key reasons. First, it makes the location of the third party, as in the Microsoft case, potentially relevant, if not determinative, of the rules that apply. This adds yet another variable, and yet another potential determinant of territoriality. It also offers a possible way to reconcile the government's position with respect to the proposed Rule 41 amendment and its position in the Microsoft case.[150] Even if law enforcement agents could not themselves access data located extraterritorially, the rules are different—or so the government says—if it is a third party doing the search or seizure.

Second, the fact of third party control once again highlights the user's lack of direct control over his or her data, and its location, at any given moment. It is, of course, possible to enter contracts with third parties ensuring that data will be stored in a particular location – and in fact, the desire to be able to control and limit the movement of one's data is what is spurring data localization movements. But most data users do not currently have such control over their data; and in fact, the efficiency of the both the cloud and an internationally-connected Internet depend, to a significant degree, on third parties being able to move around data in the most expeditious manner, without being constrained by user preferences and control.

---

[146] 442 U.S 735 (1979).

[147] 425 U.S. 435 (1976).

[148] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 35-36 (D.D.C. 2013) ("As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like. But the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people's lives.") (emphasis in original).

[149] *See, e.g.,* United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

[150] *See* discussion *supra*, Part I(C)(i).

III. WHAT DOES IT ALL MEAN?

As the preceding section highlights, data's unique characteristics raise fundamental challenges to territoriality doctrine. It does so for three key reasons: First, the arbitrariness, instability, and location independence of data and its user challenge the assumption that data location should be determinative of the rules that apply. Why should either privacy rights or law enforcement access to sought-after evidence turn on where data happens to be located at any given moment, particularly given the instantaneous, and seemingly random way in which data moves from place to place?

Second, the intermingling of data means that it is often difficult, if not impossible, to make the kind of fine-tuned distinctions that the Fourth Amendment and surveillance law's associated focus on user identity demands. Even absent the problem of multi-communication transactions, U.S. person and non-U.S. person data are inevitably intermingled by virtue of the fact that we live in an interconnected and globally networked world. Broad surveillance programs and bulk collection significantly exacerbate this problem of "incidental" collection.

Third, the location independence between the data and the government agent accessing the data creates the possibility of actors in State A searching or seizing data in State B, and doing so without any readily apparent violation of State B's territorial integrity. From the perspective of State B, however, this is a violation of sovereignty, and arguably a form of Internet bullying, with State A determining when, and according to what procedures and substantive standards, data located in State B can be seized. It ignores long-standing efforts of nations—including the United States—to establish sovereign control and regulation over data within one's own territory. In so doing, it creates a possible conflict of laws and adds fuel to data localization movements.

This section addresses what these insights mean for the three areas of law discussed in Part I—the reach of the Fourth Amendment, the scope of permissible foreign intelligence surveillance, and the territorial limits on the judiciary's warrant authority. Whereas the government continues to assume a territorial Fourth Amendment, I argue that data's mobility and interconnectedness shake Fourth Amendment territoriality at its core. Conversely, whereas the government is now arguing, at least in the context of the Microsoft case, that long-standing territorial-based limitations on law enforcement jurisdiction should yield in the face of non-territorial data, I point to countervailing policy considerations and principles of international law that, at a minimum, complicate the government's position.

As the forgoing highlights, the answers to data's un-territoriality are not, and need not be the, same across the board. But whatever one decides is the right solution, one thing is clear: highly-mobile and cloud-based data challenges the very foundation of territorial-based distinctions in the law, and these challenges need be acknowledged and addressed.

A. THE FOURTH AMENDMENT

I am not the first scholar to note the ways that data challenges a territorial Fourth Amendment. In a recent article in Stanford Law Review, Orin Kerr addresses "the clash between the territorial Fourth Amendment and the global Internet."[151] But while recognizing the way in which "Internet technologies . . . disrupt[] the prior relationship between person and place,"[152] Kerr assumes that the territorial-based distinctions announced in *Verdugo-Urquidez* are the right ones. He thus applies his Fourth Amendment theory of equilibrium adjustment—which describes and endorses a Fourth Amendment that responds to new developments in a way that maintains the status quo balance of government authority and privacy protections—to suggest a series of adjustments that will maintain the territorial and identity-based distinctions of the Fourth Amendment.[153]

I instead suggest an alternative perspective, namely that data calls into question the primacy that location has to our understanding of basic constitutional rules governing the government's authority to seize data. Even if one understands the term "the people" in the way Rehnquist suggested—limiting the Fourth Amendment's protections to citizens and those with substantial connections to the United States—the mobility and intermingling of data leave the "the people" insufficiently protected by a territorial Fourth Amendment, at least at the stage at which data is acquired.[154] This claim is even stronger if the term "the people" is, as Justice Kennedy suggested, understood to emphasize the importance of the right, rather than limit who can assert a claim. Under this view of the Fourth Amendment, the key is not whether the *particular target* of the government action is entitled to Fourth Amendment protections, but whether the government action infringes on the Fourth Amendment interests of *the people*—something that the search or seizure of intermingled data does, regardless of the location of the acquisition, location of the target, or target identity.

To be sure, Kerr himself seems to accept a key premise of my claim. He argues that, at least for cross-border communications, Fourth Amendment protections should kick in so long as *either* the sender or recipient of a communication is a U.S. person or located in the United States and thus entitled to Fourth Amendment protections under the now-dominant understanding of the Fourth Amendment's reach.[155] This is in contrast to the government's current approach, which looks exclusively at the identity and location of the *target* of the search to determine the

---

[151] Kerr, *The Global Internet*, *supra* note 12, at 289.

[152] *Id.* at 19.

[153] *Id*; *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 125 HARV. L. REV. 476 (2011).

[154] *But see* Kent, *supra* note 21, at 519 (noting that there is not any evidence of any detailed public debate about the choice of words between "person" and "the people" and suggesting that we therefore ought to be skeptical of our ability to draw much meaning from the difference in terms); Daskal, *supra* note 30 (raising concerns about Rehnquist's understanding of the Fourth Amendment's reach).

[155] *See* Kerr, *The Global Internet*, *supra* note 12, at 308-311.

applicable rules for collection, thereby effectively ignoring the privacy concerns—and potential Fourth Amendment rights—of other parties to the communication, at least at the collection stage.

The problem is, as Kerr himself acknowledges, it will not always be feasible to ascertain the location and identity of all senders and recipients of a particular communication. Kerr thus proposes a good faith standard. So long as the government makes a good faith determination of the sender and recipient's status, the search or seizure will be deemed Fourth Amendment compliant.[156] But this could become the exception that swallows the rule: How much of an effort will agents be required to make? Is a preponderance of the evidence enough?

I, instead, argue for a much stronger, albeit rebuttable presumption, that the Fourth Amendment applies: Absent clear and convincing evidence to the contrary, collection itself (irrespective of the subsequent minimization efforts) should be presumed to implicate Fourth Amendments and thus must be Fourth Amendment compliant. In other words, the Fourth Amendment protections will presumptively kick in, regardless of the location of the data or target, unless the government can convincingly established that neither the sender or recipient nor any other person with a possessory interest in the data is a U.S. citizen or person with the kind of sufficient connections to the United States to trigger Fourth Amendment protections.

Of additional concern, Kerr's proposed adjustment is, consistent with long-standing Fourth Amendment doctrine, only applicable to data in transit. It is, after all, well established that a sender's reasonable expectation of privacy in mail expires once the mail arrives at its destination.[157] At that point, the Fourth Amendment inquiry focuses exclusively on the recipient, as the sole party with a continuing reasonable expectation of privacy in the communication. Of particular importance, the law has not yet settled what it means for email—as opposed to snail mail—to reach its destination. If simply arriving at the recipient's server is what counts as "delivery" (also a possibility) then the proposed adjustment will provide little-to-no protections to a key subset of "the people" that the Fourth Amendment is meant to protect—U.S. persons sending emails to non-U.S. persons that lack Fourth Amendment rights.[158] Such communications could be seized the minute they arrived at the recipient's server, without any requirement that the government obtain a warrant, or even engage in a seizure that is reasonable.[159] Moreover, even if "delivery" is ultimately understood as

---

[156] *Id.* at 24-27.

[157] *See* 4 Wayne R. LaFave, *Search and Seizure,* § 11.3(f) (1987); United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (citing cases).

[158] Kerr acknowledges this problem. *See* Kerr, *The Global Internet*, *supra* note 12, at 315 (noting that if arrival at the server constitutes delivery, "the government will be able to freely monitor the e-mail account of a person who lacks Fourth Amendment rights under *Verdugo-Urquidez* regardless of whether that person communicates with those who have Fourth Amendment rights").

[159] If done for the explicit purpose of gathering U.S. person data, this would be impermissible as an example of reverse targeting. Notably, in recent litigation, the Justice

receipt by the intended recipient (and not just arrival on the recipient's server), the sender would still lack any Fourth Amendment interest in the information once it has been opened or downloaded onto the recipient's device. My proposed rule, by contract, assumes that Fourth Amendment requirements apply whenever such data implicates Fourth Amendment interests, and thus would apply Fourth Amendment requirements to the collection of a communication from a U.S. person to a non-U.S. person, even if the communication had been downloaded and read by the non-U.S. person recipient.[160]

Thus, even with the kind of helpful adjustments suggested by Kerr, the intermingling of U.S. and non-U.S. person information create a significant possibility of both error and "incidental collection." Put another way, a territorial Fourth Amendment, even as adjusted, fails to provide the kinds of Fourth Amendment protections it promises to "the people" it is meant to cover.

I, instead, suggest a very different test: one in which the Fourth Amendment is presumed to apply, regardless of whether the collection takes place within the United States or outside the United States, and regardless as to whether or not the target is a U.S. person or not. The presumption can be rebutted if and only if the government establishes that *none* of the parties to the communication or with some kind of ownership interest in a particular document are U.S. persons (those entitled to Fourth Amendment rights). In practice, this means that bulk collection, wherever it takes place, will fall within the Fourth Amendment's ambit; cross-border communications will be presumptively be covered by the Fourth Amendment, irrespective of the identity of the particular target; and most foreign intelligence surveillance will also trigger a Fourth Amendment inquiry, as it will not be feasible in most cases to make the showing that none of the interested parties have Fourth Amendment rights. By contrast, the surveillance of North Korean diplomats in North Korea will not likely trigger the Fourth Amendment—although there may be policy reasons to expand protections across the board, even in these circumstances.

To be clear, this is not the same as saying that a warrant is required every time the government searches or seizes electronic communications for foreign intelligence purposes, or that all surveillance necessarily implicates the Fourth Amendment. I am, in fact, persuaded by the notion of a foreign intelligence exception to the warrant requirement, but have concerns about how broadly the exception has been defined—a topic for yet another

---

Department has helpfully hinted that the destination point is receipt by the actual recipient, not just arrival at the ISP, which means that the sender retains a reasonable expectation of privacy until it is actually received by the recipient. *See* Government's Unclassified Response to Defendant's Alternative Motion for Suppression of Evidence & a New Trial at 25-31, United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014), 2014 WL 4972313, *48 n.32.

[160] This would, of course, require a rethinking of established doctrine, or at least an acknowledgment that it applies differently in a digital age. But the Supreme Court has indicated a willingness to do just that in light of some of the novel issues presented by new technology. *See, e.g.,* Riley [add cite].

project. What I am saying is that the Fourth Amendment protections, however defined, ought to be applied to U.S. person targets and non-U.S. person targets alike, absent a determination by clear and convincing evidence that collection does not encompass communications that are to or from a U.S. person, and does not include other data, such as stored documents, that have been generated in whole or part by a U.S. person.

To be more concrete: If a warrant based on probable cause is required to collect the content of certain types of electronic communications, it should be required irrespective of the location of the data or the target, and irrespective of whether the target is a U.S. person or non-U.S. person, absent a determination that the communication is between non-U.S. persons only. Conversely, if a warrant is not required to collect certain types of information, such as phone numbers dialed or the to/from line of an Internet communication, this too should apply across the board, to citizens and non-citizens alike, regardless of where the data or target is located—absent a determination that the communication is between non-U.S. persons only.

Such a proposal will undoubtedly engender objections. It would be, after all, a dramatic change in the way the government thinks about the obligations of the U.S. government with respect to its treatment of non-U.S. persons outside the United States. But the United States is already moving in that direction, albeit as a matter of policy, not law. A recently issued President Policy Directive (PPD-28), which directs the intelligence community to establish post-acquisition limits on dissemination and retention of collected data, requires that these safeguards apply "equally to the personal information of all persons regardless of nationality," to "the maximum extent feasible consistent with national security."[161] The policy directive applies across the board, even in those situations where all parties to a communication are non-U.S. persons.

Many will nonetheless object that interposing the Fourth Amendment as constraint on the collection of non-citizens data overseas will unduly burden the U.S. government, impeding the ability to gather critical foreign intelligence information and therefore imperiling the nation. And that minimization rules are sufficient to address the Fourth Amendment concerns I have identified. But as already described, the Fourth Amendment need not—and in fact does not—act as a chokehold with respect to the gathering of foreign intelligence information. The Fourth Amendment's reasonableness requirement—described as the

[161] *See* PPD-28, *supra* note 17, § 4(a). *See* David Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SEC. L. & POL'Y, 209, 289 (describing PPD-28 as representing an "unprecedented change in U.S. intelligence policy, at least at the rhetorical level," but noting that "[t]he degree of substantive change that will follow from PPD-28 is less certain"); Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), http://www.lawfareblog.com/2014/01/the-presidents-speech-and-ppd-28-a-guide-for-the-perplexed.

"touchstone" of Fourth Amendment analysis[162]—is a quite flexible standard that balances the government and privacy interests at stake, generally giving significant weight to the former. Even in the context of domestic law enforcement, where Fourth Amendment interests are at their zenith, the doctrine has generally been permissive, giving law enforcement agents significant latitude to search and seize. Searches targeting non-citizens will still permit the government to engage in a wide array of law enforcement and intelligence activities; it will simply prohibit *unreasonable* seizures of data as a means of indirectly protecting "the people" that fall within the Fourth Amendment's ambit.

Moreover, while minimization rules are important, and deserving of much more attention from Congress (and academics) than it has received to date, the interests are separate. Collection governs the government's authority to gather information. Minimization governs what the government can do with it once it has it in its hands. As already stated, Congress has almost exclusively focused on collection—based on what I deem an implicit understanding that the collection itself poses a potential harm that requires regulation, even if only a consequentialist one. This, in my view, is correct. While restrictions on use, dissemination, and retention of information already collected minimize (hence the term) the consequential harms that might flow from collection, the two steps should be analyzed separately. Unless the government were to purge all collection that implicates U.S. persons—which it does not and should not—collection changes the balance of power between the individual and the government and thus implicates the Fourth Amendment rights of "the people." Collection should thus be understood as an independent Fourth Amendment event and regulated accordingly.

To reiterate, I am not saying all electronic surveillance or seizure of data triggers the Fourth Amendment. Nor am I saying that a warrant is required any time the Fourth Amendment is triggered. There is an important and ongoing debate about when and in what circumstances the Fourth Amendment protects electronic communications and other types of data.[163] Among the many unresolved questions are the dividing line between metadata and content information, the extent to which that line matters, and the scope of the third party doctrine. My point is simply that whatever answers we arrive at, they ought to apply equally to U.S. persons and non-U.S. persons, regardless of whether the target of collection and data being collected is based in the United States or not—absent a

[162] *See, e.g.,* Bringham City v. Stuart, 547 U.S. 398, 403 (2006) ("The ultimate touchstone of the Fourth Amendment is reasonableness.")

[163] The government, for example, continues to argue that the Fourth Amendment does not protect the contents of email held by an ISP, although the weight of authority suggests otherwise. *See supra* note 99. *See also United States v. United States District Court* (Keith), 407 U.S. 297, 308-09 (1972) (explicitly leaving open the possibility of a foreign intelligence exception to the warrant requirement); *In re Directives,* 551 F.3d 1004, 1012 (FISC Rev. Ct. 2008) (holding that "a foreign intelligence exception to the Fourth Amendment's warrant requirement exists" in specified circumstances).

determination that all parties to the communication are non-U.S. persons. In many cases non-citizens will be entitled to the protections of the Fourth Amendment—not because they are subsumed within "the people," but as a means of protecting citizens and other persons with sufficient connections to the United States that the dominant theories of constitutional interpretation tell us are entitled to the Amendment's protections.

B. FOREIGN SURVEILLANCE: ADDITIONAL CONSIDERATIONS

Recommendations with respect to the statutory requirements governing foreign intelligence surveillance track—as they must—those made with respect to the Fourth Amendment. The insight of the 1978 Congress is prescient in this regard: The best way to ensure sufficient protections for Americans is to provide sufficient protections for all, at least at the collection stage. The insight has only proved to be more salient over time, as the Internet has become truly global. Congress should thus re-write FISA to set universally applicable requirements for acquisition that no longer depend on the location of the data, or location or identity of the target.

Again, my purpose here is not to identify the specific rules that ought to be adopted—a topic that deserves its own article. Perhaps warrants should be required. Or perhaps not. Or perhaps there is a middle ground, in which warrants are required for certain types of acquisition, or acquisition done for specified purposes. But whatever the rules, they ought to depend on the nature of collection (*i.e.,* the type of data being collected) and the purpose of collection (*i.e.* whether the primary purpose is foreign intelligence or whether the primary purpose is law enforcement), and then applied universally, regardless of the location of the data, location of the target, or identity of the target. Notably, the broader the definition of foreign intelligence, the harder it is to justify a warrant exception for foreign intelligence surveillance; as the definition is narrowed and limited, then support for warrantless surveillance is more justifiable. The applicable definitions and the procedures provided ought to be considered and evaluated jointly.

At the same time, Congress should focus more directly on the critically important—and largely neglected—question of use.[164] Who can access the data? Based on what substantive and procedural rules? In what circumstances can data be disseminated? How long can the data be retained? As of now, the statutory scheme is focused almost entirely on the rules governing collection and gives scant attention to the important questions about how data that has been collected is to be accessed and used. Congress, for example, requires the existence of minimization rules with

[164] *See also* Banks, *supra* note 10, at 1660 (noting that "[b]y its nature, the FAA shifts nearly all the burden of civil liberties protection to postcollection minimization," and urging Congress to legislate more robust minimization requirements).

respect to the accessing, retention, and dissemination of U.S. person information, but then delegates development of "specific procedures" to the Attorney General, subject to approval by the FISC. The overarching requirements are written at such a level of generality that they effectively delegate all the key details to the executive.[165] This is a mistake.

A recently issued President Policy Directive (PPD-28) similarly emphasizes the importance of post-acquisition limits on dissemination and retention of collected data, and directs the intelligence community to establish additional post-acquisition safeguards for personal information collected from signals intelligence (which includes electronic communications). Interestingly, it requires that these safeguards apply "equally to the personal information of all persons regardless of nationality," to "the maximum extent feasible consistent with national security."[166]

Congress should engage as well, and not leave the elaboration of future use restrictions solely to the executive branch. Even with enhanced protections derived from the Fourth Amendment, foreign intelligence collection is likely to be sweeping. As a result, minimization rules and use restrictions will continue to be critical. And while this article (like Congress) is focused primarily on collection and does not purport to make specific recommendations as to their content, it would be amiss to ignore their importance. Meanwhile, Congress ought embrace the reality of data's intermingling, and rewrite its collection rules to turn on the nature and purpose of collection, not the identity or location of the target.

C. THE MICROSOFT CASE: WARRANT JURISDICTION AND THE STORED COMMUNICATIONS ACT

Territoriality with respect to warrant jurisdiction serves a very different purpose than it does in the Fourth Amendment context. Whereas territoriality under the Fourth Amendment demarcates who is—and is not—entitled to basic privacy protections vis-à-vis the U.S. government, territoriality for purposes of warrant jurisdiction defines the geographic scope of court-approved law enforcement authority to act. Territorial-based limitations for purposes of warrant jurisdiction stem from the long-standing principle that nations are prohibited from exercising unilateral law enforcement jurisdiction in another nation's territory, as well as an awareness of the diplomatic consequences and practical difficulties of doing so.

---

[165] *See* 50 U.S.C. § 1801(h) (2010)(defining the required "minimization procedures")

[166] *Id.* § 4(a). *See* David Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SEC. L. & POL'Y, 209, 289 (describing PPD-28 as representing an "unprecedented change in U.S. intelligence policy, at least at the rhetorical level," but noting that "[t]he degree of substantive change that will follow from PPD-28 is less certain"); Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), http://www.lawfareblog.com/2014/01/the-presidents-speech-and-ppd-28-a-guide-for-the-perplexed.

Notably, both sides in the Microsoft case argue that they respect the territorial-based limits on the government's warrant authority. They just differ as to the question of what is territorial and what is extraterritorial, at least for purposes of the Stored Communications Act. Microsoft argues by analogy to the territorial-based limits applicable to warrants issued under the Federal Rules of Procedure 41 and rules governing the search and seizure of tangible property. According to Microsoft, it would be an extraterritorial seizure if the government accessed the data directly; thus, it remains an extraterritorial seizure if instead of seizing the data directly, the government compels Microsoft to do so.[167] The government, by contrast, points to the text and structure of the Stored Communications Act to suggest that the term "warrant" in the Stored Communications Act is actually part warrant and part subpoena. By analogy to rules governing subpoenas, it is, according to the government, the location of the entity (Microsoft) with control over the data that counts.[168] Both sides cite policy reasons as to why their interpretation is the right one.

The case thus pits data location against the location of access, requiring an answer as to which controls, at least for purposes of warrant jurisdiction under the Stored Communications Act. Purely from a policy perspective, both sides have strong claims—and neither approach is fully satisfactory.[169] Microsoft's position, in which law enforcement access to evidence depends on the location of data yields bizarre results, under which law enforcement access to evidence depends on ISP's decisions about the most cost-effective and efficient storage location at any given moment. Nefarious players could manipulate data location to their advantage, seeking out companies that store data in nations unwilling, or perhaps technologically unable, to cooperate with official government-to-government requests for electronic evidence. ISPs may also have business incentives—based on customer demand—to move data to locations where cooperation with U.S. law enforcement is minimal, thus creating significant barriers to the investigation of crime.

---

[167] In support of this position, Microsoft emphasizes that Congress's use of the word "warrant" should be understood to mean what it says and not "subpoena" or some hybrid warrant-subpoena as the government suggests. *See* Brief for Appellant, *In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft, no. 14-2985-CV (2d Cir. Dec. 8. 2014)[hereinafter Appellant Brief, Microsoft] at 37 ("The notion that Congress used the word 'warrant' to mean 'subpoena' (or 'something like a subpoena') is inconsistent with the statute's text.")

[168] *See* Appellee Brief, Microsoft, *supra* note 1, at 9; *see also In re* Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft*,* 15 F. Supp. 3d at 471 ("Although [the Stored Communications Act] uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena.")

[169] The textual and structural claims are of obvious import as well. Microsoft makes a strong case that, given Congress's silence on the issue, the statute ought to be construed in accordance with international law. And as stated above, international law is widely understood to prohibit the kind of unilateral exercise of law enforcement in another state's territory that the government's position would permit. See Appellant Brief, Microsoft, *supra* note 161, at 34-35.

But the government's answer—that the location of access controls—seems to create as many problems as it solves. It generates a system of borderless law enforcement, but without agreed-upon standards and procedures. The standards and procedures of the requesting state (the United States in this case) are effectively imposed on the state where the data is stored (Ireland), without consideration of the applicable privacy protections and rules governing law enforcement access to data in the state where the data is located. This has several negative policy implications.

First, it conflicts with the international law restrictions on the unilateral exercise of extraterritorial law enforcement jurisdiction and ignores long-standing principles of international comity. This is not just a matter of abstract principle, but stems from the long-standing sovereign interest in setting privacy protections for those within the nation's territory, as well as respect for differences in how privacy is treated across jurisdictions. Second, and relatedly, there is a legitimate concern about the reciprocal effects on the United States' ability to safeguard stored data held within the nation's borders, including the data of its own citizens. The United States' position may seem the correct one when it is U.S. law enforcement accessing the data, and the data is being accessed for legitimate law enforcement needs pursuant to a finding of probable cause. But what happens when another nation, such as China or Russia, seeks to compel a service provider operating within its territorial borders to turn over data stored within the United States regarding a dissident human rights activist?[170] Or consider the likely scenario of UK law enforcement, pursuant to newly enacted authority, seeking to compel ISPs to directly turn over data stored in the United States, without regard to ECPA.[171]

Third, such a scenario—with both the requesting state and state where data is stored claiming an interest in the data—creates an almost inevitable conflict of laws. ISPs are thus caught between two conflicting legal obligations, perhaps even with criminal law consequences. While this is not new—and there is an entire body of law designed to deal with such conflicts problems—it does put ISPs in an unenviable position; [172] the fact that the problem is not novel problems does not mean it should be encouraged. Fourth, the U.S.'s insistence that it can compel U.S.-based ISPs to produce their customer's data, wherever located and without regard to

---

[170] *Cf.* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORD. INTELL. PROP. MEDIA & EN. J.J. 567, 582 (2012) ("The geographically unlimited regulation and enforcement of cyberlaw 2.0 has been liberating only when it is 'our' laws that are being enforced; as soon as other countries enforce 'their' laws that are contrary to our beliefs, we begin to look for ways to protect our own value system.")

[171] *See* Data Retention and Investigatory Powers Act, 2014, §4(4), *supra* note 106. The legislation specifies that "regard is to be had" to a possible conflict of laws, although the legislation does say whether and in what situations the laws of the nation in which the data is located would trump. *Id. See also* INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, REPORT ON THE INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY 2014, H.C. 794, at 151 (describing a key goal of the legislation as permitting access to otherwise difficult-to-obtain data held by U.S.-based providers)

[172] [Add cites to conflict literature.]

the laws where the data is stored, fuels data localization movements, with negative repercussions both for U.S. business and the growth of the Internet as a whole.[173] The economic fallout of such movements is potentially significant, with costs to U.S. business potentially high.[174] More importantly than the parochial interests of the U.S. businesses, such localization movements also undercut innovation and minimize the efficiency and effectiveness of the cloud. Ironically, if such movements are ultimately successful in creating closed off networks, law enforcement access to sought-after data will suffer. The very thing that the government is seeking to do in the Microsoft case—compel a US-based ISP to turn over data located extraterritorially—will be impossible, because that data will be held in closed-off networks. Stated another way, the government's insistence on unilateral access to the data may make its ability to ever compel such data more difficult, despite the potentially legitimate interests in doing so.

Taken together, these concerns highlight both the need for new cross-border mechanisms for accessing data and the importance of respecting the sovereign interest in setting privacy protections and controlling law enforcement access to data stored in a non-transitory way within one's jurisdiction.[175] There are several ways to achieve this balance. Here I discuss four.

The first option is simply to strengthen the Mutual Legal Assistance Treaties system, pursuant to which law enforcement officials can make

---

[173] *See* Hill, *supra*, note 105.

[174] In response to revelations about the scope of U.S. foreign intelligence surveillance, the government of Germany has announced plans to cancel a contract with Verizon*;* Brazil has abandoned a plan to use Microsoft Outlook for government email; and Brazil and the European Union have decided to build their own cables between Brazil and Portugal. *See* Anton Troianovski & Danny Yardon, *German Government Ends Verizon Contract*, WALL ST. J., June 26, 2014, http://online.wsj.com/articles/german-government-ends-verizon-contract-1403802226; Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies,* N.Y. TIMES, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0. A recent report suggested that concerns about U.S. surveillance practices could cost U.S. technology companies $22 to 35 billion over the next three years as foreign customers abandon or choose U.S. providers. *See* Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry*, THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Aug. 2013), http://www2.itif.org/2013-cloud-computing-costs.pdf; Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute (July 2014), http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf. While these reactions have been motivated to date by the scope of foreign intelligence surveillance, a rule that U.S. law enforcement can unilaterally reach into other nation's jurisdictions is likely to exacerbate this problem.

[175] *See, e.g.* Brad Smith, *Time for an International Convention on Government Access to Data,* MICROSOFT DIGITAL CONSTITUTION (Jan. 20, 2014), http://digitalconstitution.com/time-international-convention-government-access-data/

formal requests for cross-border law enforcement assistance.[176] It is, after all, Microsoft's position is that the government is obliged to go through the Mutual Legal Assistance Treaty with Ireland to request the sought-after data, and that its failure to do so may itself be a violation of international law. This is also Ireland's position.[177] But the MLAT system has historically been slow and clumsy, which is precisely why the government is seeking to get the data directly from the ISPs. The United States, example, takes an average of ten months to respond to law enforcement requests made to the United States pursuant to the MLAT process; other nations take much longer.[178] Moreover, MLAT coverage is not universal; the United States for example has MLATs with only about half the countries in the world. That said, the processes can, and clearly should be, improved. International cybercrime treaties, for example, provide a mechanism for nations to expedite and facilitate preservation orders and cross-border sharing of information; these can be expanded to cover other criminal matters as well. Increased resources, both money and personnel, is also needed.

That said, while there are a myriad of reasons why it would be a good idea to strengthen the MLAT system, such a system—even a greatly improved one—does not adequately respond to the government's legitimate concerns. Such a system still depends on the need to isolate and locate the data at any given point in time—something that may be increasingly difficult, if not impossible, to do. It also depends on the recipient state receiving and agreeing to the requesting state's demands.

A second, alternative approach might rely on the MLAT process (ideally strengthened) in the majority of cases, yet also permit the issuance of warrants with extraterritorial reach based on some sort of extraordinary circumstance certification by the Attorney General or his or her designee—*i.e.*, based on exigent circumstances or a finding that there is no effective bilateral process in place for preserving and responding to U.S. demands for evidence. This has the advantage of continuing to respect sovereign interest in control over data in the run-of-the mill case, but also providing a more expedient means of getting the data when exigent circumstances demand it. Importantly, the decision to bypass the MLAT process is put in the hands of a named executive branch official, rather than the courts. This matters. The decision to trump another nation's sovereign interest ought be made by the executive branch, after consideration of any diplomatic or broader policy implications, rather than the hundred-plus magistrate and state court judges authorized to sign off on ECPA warrants.

---

[176] *See, e.g.,* Global Network Initiative, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE (released Jan. 2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.

[177] *See* Brief of Amicus Curiae Ireland, *supra* note 110, at 4.

[178] *See, e.g.,* THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATION TECHNOLOGIES, *Liberty and Security in a Changing World*, WHITE HOUSE 226-229 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records and recommending that the United States streamline and improve the MLAT process).

Yet a third option is that reflected in legislation introduced in the last Congress by Senators Orrin Hatch (R-UT), Chris Coons (D-DE), and Dean Heller (R-NV). The legislation, titled the Law Enforcement Access to Data Stored Abroad (LEADS) Act, authorizes the issuance of ECPA warrants with extraterritorial reach, but only when the target is a U.S. person, defined as a U.S. citizen or legal permanent resident.[179] If enacted, it would set the precedent that states can unilaterally compel the extraterritorial production of their own citizens' and legal permanent residents' data, but could not compel the data of other non-citizens located extraterritorially. Such an approach respects the sovereign interests of other nations' in controlling access to their own citizens' data located within their territory, thus protecting against other nations seeking to compel production of U.S. person data stored in the United States. Moreover, the legislation provides a mechanism for quashing a production order if it would violate the laws of a foreign nation, thereby protecting ISPs from being caught between two irreconcilable legal obligations.[180]

While definitely a step in the right direction, the legislation suffers from some of the same identification problems discussed in Part II. The government is permitted to obtain U.S. person data pursuant to a warrant, but what happens if neither law enforcement nor the ISP knows the identity of the target? One could imagine a situation in which unknown targets are addressed through a series of presumptions that, while perhaps accurate in a majority of cases, are hardly foolproof. And what if they get it wrong? Ordinary good faith principles would presumably apply, but again, depending on how good faith is defined, the exception might swallow the rule. Or what if multiple persons have an interest in the data? Whose citizenship status controls?[181]

The best option, but also the hardest to institutionalize, at least in the short term, would be some sort of international agreement that permits governments to access, or compel the production of sought-after data wherever located, but pursuant to agreed upon substantive and procedural standards. This could be achieved in a number of ways. A supra-national warrant system is one possible model, but also near impossible to

---

[179] S. 512, 114th Cong. (2015).

[180] Orin Kerr similarly has suggested that the territorial scope of ECPA should depend on user location. Kerr, *The Next Generation, supra* note 10, at 416. But Kerr seems to contradict himself two years later, when he writes, albeit with respect to the scope of the Fourth Amendment as opposed to the SCA, that "it is preferable for Fourth Amendment standards to follow the location of the information instead of the person." He points to, among other concerns, the difficulty of identifying person location, and the problems that would arise when multiple people, some located territorially, some extraterritorially, have a Fourth Amendment interest in the data being seized. Kerr, *The Global Internet, supra* note 12, at 322-24.

[181] *See id*; s*ee also* Greg Nojeim, *LEADS Act Extends Important Privacy Protections, Raises Concerns,* CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 18, 2014), https://cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/(noting the anomalies that would be created by treating U.S. person and non-U.S. person data differently).

institutionalize. Among the many questions: Who issues the warrant? Based on what standards and procedural effects? How would wildly divergent legal systems be reconciled to achieve consensus on these difficult issues? Another option would be some sort of formal treaty that would specify when and under what circumstances one government could directly compel an ISP to turn over data, irrespective of its location. While this avoids some of the logistical and structural issues associated with the development of a new global warrant system, it still raises the same range of highly contested substantive and procedural questions as to for what purposes and based on what processes a governments can search and seize.

An alternative, and perhaps more promising approach to start, might be a set of more informal agreements—almost like best practices across a group of like-minded nations—that would specify when and under what circumstances governments could be permitted to directly compel the production of communications data from ISPs and other similarly situated providers, thus beginning to address some of these contested issues. The range of informal, but highly effective, mechanisms for regulating global financial transactions provides one possible model.[182]

Such an internationally-agreed upon system allowing direct cross-border access to data would, regardless of specific form, produce the same effect as what the government is seeking in the Microsoft case, but would do so based on sovereign consent. Properly designed, it would address the arbitrariness and instability of data location, while also avoiding the negative consequences that the unilateral exercise of law enforcement authority yields. Companies would no longer be caught in a conflict of laws; data localization efforts would lose steam, at least in the countries that signed on to the global warrant system, as locally kept data would be subject to searches and seizures as internationally-connected data; and assuming the system had a sufficiently large reach, companies would no longer be under pressure to enter contract of service agreements that limited where they could store or move data, with benefits to both law enforcement and the efficiency and development of the Internet as a whole.

Implementation would no doubt be complicated and would need to start slow, presumably among a handful of nations—with input from the ISPs and other key stakeholders—that operate with a mutual respect for one another's judicial system and the ability to agree upon, apply and enforce the substantive and procedural rules and privacy protections. But while not something that can be implemented overnight, the increasingly close intelligence cooperation across partner nations, as well as the increasing density of international institutions with jurisdiction to opine on, if not enforce, issues once the exclusive province of sovereign nations, means that such an internationally agreed upon system is not as far-fetched as it might

[182] Add CITES/DISCUSSION

initially appear. In fact, recent reporting suggests it is something that nations with key stakes in these issues are already exploring. [183]

Finally, an institutional point: whatever one decides is the best approach – an updated MLAT system, ECPA warrants with extra-territorial reach, or a new internationally agreed upon system--the policy and diplomatic reverberations will be global. These are decisions that should be made by the political branch, not unelected federal judges. It is Congress's job to update the statute, and the executive's responsibility to negotiate new international agreements—not the courts' job to rewrite ECPA to accommodate concerns not referenced or even conceivable to its drafters. Put bluntly, the Second Circuit, in its consideration of the Microsoft case, should reject the kind of unilateral statutory update that the magistrate and district court have advocated.

The short-term result is concededly imperfect. Territoriality for purposes of warrant jurisdiction, whether pursuant to FRCP 41 or ECPA, will continue to be determined by data location—at least until Congress passes new legislation or the executive negotiates new agreements. That said, the government is not hapless in the interim. To the contrary, agents seeking data located in another nation generally will still be able to get it. They just need to go through formal channels, albeit often clumsy and time-consuming, as would be required if they were seeking access to tangible property. And if the executive decides that process is too cumbersome in a particular case, it presumably can find ways to ignore or subvert it. There are, after all (and as the Snowden revelations have made all too clear), multiple tools available for acquiring extraterritorially located data without the consent of the nation where the data is stored—some covert, some overt. But such a decision to override treaty and international law obligations regarding respect other nations' sovereignty is something that should be decided by the political branches, not the hundreds of magistrates and state court judges across the country.

In sum, law enforcement access to data should no longer depend on where the data is located at any given moment. But this move toward borderless law enforcement should be based on mutually agreed upon standards and procedures—not based on which governments control which entities at any given moment. And not based on a court decision that fails to take into account the broader policy considerations at play.

CONCLUSION

Data is shaking territoriality at its core. Whereas territoriality depends on the ability to define the relevant "here" and "there," data is everywhere and anywhere, and calls into question what "here" and "there" matter. This article exposes the ways in which data undercut long-standing assumptions about the territorial reach of the Fourth Amendment, the

[183] *See, e.g.,* http://www.theguardian.com/world/2015/jun/02/web-firms-data-sharing-secret-treaty

viability of territorial-based distinctions in surveillance law, and territorial limits to judges' warrant authority. But just as the challenges posed by data are multi-layered and complex, so are the solutions.

To date, the government has gotten it precisely backwards. Territorial-based distinctions embedded in the Fourth Amendment and the statutory-based surveillance scheme governing electronic surveillance fail to serve the very interests they are designed to protect. Such distinctions should be eliminated, at least with respect to the seizure of data. At the same time, courts should at least in the short-term continue to respect territorial-based limitations with respect to law enforcement jurisdiction, thereby giving Congress time to engage and the executive the time needed to achieve international consensus on a new approach.