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 relevant "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 addresses these challenges. It explores the unique features of data, and highlights the ways in which data undermines longstanding assumptions about the link between data location and the rights and obligations that should apply. Specifically, it argues that a territorial-based Fourth Amendment fails to adequately protect "the people" it is intended to cover. Conversely, 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 William Banks, Bobby

INTRODUCTION

In December 2013, United States federal law enforcement agents served a seemingly innocuous search warrant on Microsoft, demanding information associated with a Microsoft user's web-based email account. But there was only a problem—the emails sought by the government were located in a data-storage center in Dublin, Ireland. Consequently, Microsoft refused to turn over the emails, claiming that the government's warrant authority did not extend extraterritorially; the warrant was therefore invalid. The government, along with the magistrate judge and district court, disagreed—concluding that the relevant reference point for purposes of warrant jurisdiction was the location of the provider (in this case Microsoft), not the location of the data.[1] Because the Ireland-based data could be accessed and retrieved by Microsoft employees within the United States, the warrant was territorial—not extraterritorial—and 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, and is now being litigated before the Second

[1] *See 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) [hereinafter *Microsoft*]. The case is now pending before the Second Circuit. *See* Brief for Appellee, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Mar. 9, 2015) [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 of Oral Argument, *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. Apr. 25, 2014) (No. 13-MJ-2814). [hereinafter Oral Argument Tr., Dist. Ct., *Microsoft*]..

[2] *See Microsoft*, 15 F. Supp. 3d at 476 (concluding that warrant "places obligations only on the service provider to act within the United States"); Appellee Brief, *Microsoft*, *supra* note 1, at 32-33 (rejecting the claim that there is anything extraterritorial about Microsoft being compelled to disclose to U.S.-based law enforcement officials records under its control); Transcript of Oral Argument, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., (2d Cir. Sep. 9, 2015) (No. 14-2985-CV) [hereinafter Oral Argument Tr., 2d Cir., *Microsoft*], at 63.

Circuit. It has garnered the attention of communication companies throughout the United States, the Irish government, 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[4]—a sentiment echoed in the amicus briefs supporting Microsoft.[5] But this 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?

The dispute lays bare the extent to which modern technology challenges basic assumptions about what is "here" and "there." It challenges the centrality of territoriality within the relevant statutory and constitutional provisions governing the search and seizure of digitized information. After all, territorial-based dividing lines are premised on two key assumptions: that objects have an identifiable, and stable location, either within the territory or without; and that 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 data flows across borders make its location 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's location.

---

[3] Amici on behalf of Microsoft in the Second Circuit include a list of the who's who from the telecommunications industry, including Apple, Amazon.com, Accenture, AT&T, Verizon, Cisco, Hewlett-Packard, and eBay; 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, National Public Radio, and the Washington Post; the Government of Ireland; 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/ [http://perma.cc/D8FC-9Z4H]. *See also* Editorial, *Adapting Old Laws to New Technologies: Must Microsoft Turn Over Emails on Irish Servers?*, N.Y. TIMES (July 27, 2014), http://www.nytimes.com/2014/07/28/opinion/Must-Microsoft-Turn-Over-Emails-on-Irish-Servers.html [http://perma.cc/R8JD-V3WT]; Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST: THE VOLOKH CONSPIRACY (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 [http://perma.cc/YUG5-DWKX]. Communication companies warn of a devastating loss of business if the government prevails.

[4] Letter from Viviane Reding, Vice-President, European Comm'n Justice, Fundamental Rights and Citizenship, to Sophie in 't Veld (June 24, 2014), http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-.pdf [http://perma.cc/A4V5-NLXX].

[5] *See , e.g.,* Brief of Amicus Curiae Anthony J. Colangelo, Int'l Law Scholar, in Support of Appellant at 18-19, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) (warning that execution of the warrant would violate Ireland's sovereignty and therefore constitute a breach of international law); Brief of Amici Curiae Digital Rights Ireland Ltd., et al. in Support of Appellant at 24-25, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) (arguing that a decision to bypass the Mutual Legal Assistance Treaty in place between the United States and Ireland violates the United States' treaty obligations and is "contrary to law and precedent").

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 be, 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 that affect 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 with a particular email account).[6] 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; they call into question the normative significance of longstanding 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 noncitizens 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.[7] Conversely, the Fourth Amendment does not protect noncitizens outside the United States, absent sufficient voluntary connections to the nation.[8] Thus, territoriality doctrine, at least

---

[6] In making this claim, I assume that the author of a document or email retains a reasonable expectation of privacy in the data, even if stored by a third-party provider. This is obviously a contested claim. *See, e.g.*, Sherry Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 126-30 (2002) (noting and critiquing the doctrine that information exposed to third parties loses its reasonable expectation of privacy); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L. J. 1087, 1118 (2006) (warning that under current doctrine a "wide variety of ostensibly confidential information shared with third parties . . . remain outside the protection of the Fourth Amendment" and that statutory protections are "piecemeal and inconsistent").

[7] *See, e.g.*, Reid v. Covert, 354 U.S. 1, 64 (1957) (extending jury trial rights to civilian dependents of the military located abroad); Memorandum from David J. Barron, Acting Assistant Att'y Gen., Office of Legal Counsel, U.S. Dep't of Justice to the Att'y Gen., Re: Applicability of Federal Criminal Laws and the Constitution to Contemplated Lethal Operations Against Shaykh Anwar al-Aulaqi 38 (July 16, 2010), http://www.justice.gov/sites/default/files/olc/pages/attachments/2015/04/02/2010-07-16_-_olc_aaga_barron_-_al-aulaqi.pdf [http://perma.cc/T55C-CVSW] [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.").

[8] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) ("'[T]he people' protected by the Fourth Amendment . . . refers to a class of persons who are part of a national community or who

for constitutional purposes, involves a two-part inquiry into territoriality and target identity—with target identity turning on the depth of the target's connections to the United States.

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 also exposes the problems with making identity determinative of such rights and obligations. Digital footprints are neither observable nor readily identifiable 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 the user'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 connection to the United States.[9] While similar identification problems occur in the world of tangible property, the ubiquitous and intermingled nature of data compounds the problem of identification in both degree and kind. This problem is particularly acute in the context of mass surveillance, where the sheer quantity of data collected necessitates 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 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 threefold: first, to expose the fiction of territoriality in a world of highly mobile, intermingled, and divisible data; second to highlight flaws in the territoriality doctrine; and third, to suggest alternative approaches to thinking about the scope of the Fourth Amendment, the rules governing the acquisition of foreign intelligence information, and the territorial limits on law enforcement jurisdiction.

In so doing, this Article fills an important gap in the literature. While there was a surge of scholarship in the 1990s on the borderless Internet's effect on sovereignty, the literature focused primarily on e-commerce and emerging private law issues that were largely resolved through the harmonization of business practices.[10] By comparison, scholarly literature has devoted comparatively little

---

have otherwise developed sufficient connection with this country to be considered part of that community.").

[9] *See, e.g.*, Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST (Dec. 6, 2013), http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html [http://perma.cc/JZ2T-CPHW] (describing the difficulty of determining the identity and location of a known Internet user); Letter from Mythili Raman, Acting Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 2 (Sept. 18, 2013), https://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [https://perma.cc/MC3X-RPYH] [hereinafter Raman Letter] (describing the increased use of sophisticated anonymization technologies).

[10] *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006); Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311 (2002); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace,* 48

attention to the constitutional and sovereignty implications of the government reaching or sending its agents across borders to search and seize. Orin Kerr offers perhaps the most sustained attention to the issue, but he does so while focusing primarily on border searches and, relevant to this Article, while maintaining the Fourth Amendment's territorial-based distinctions.[11] I, by contrast, argue that data challenges territoriality doctrine at its core, requiring us to reconsider—and in some cases reject—the territorial-based distinctions as they apply to the search and seizure of digital data.

The Article proceeds in three parts. Part I begins by analyzing the longstanding presumption against extraterritoriality, examining its dominant (and often confused) constitutional, statutory, and jurisdictional applications. It explores the underpinnings of the now-dominant view that only certain "people"—namely U.S. citizens, noncitizens with substantial voluntary connections to the United States, and those physically present in the United States—are entitled to Fourth Amendment rights and heightened statutory protections with respect to foreign intelligence surveillance

This section also highlights the very different purposes served by territoriality in the context of the Fourth Amendment doctrine (and by extension surveillance law) and territoriality for purposes of warrant jurisdiction. The Fourth Amendment imposes *restrictions* on the government's authority to search and seize; by contrast,, warrants provide the government the affirmative *authorization* to do so. Thus, whereas territoriality for Fourth Amendment purposes is based on an understanding of who is entitled to privacy rights vis-à-vis the U.S. government., territorial-based limits on warrant jurisdiction are based on respect for other nations' sovereignty coupled with pragmatic concerns about the difficulty of unilaterally enforcing a warrant within another nation's borders.

Part II highlights the ways in which data challenges key underlying presumptions about territoriality across each of these areas of the law. This section identifies central differences between data and its tangible counterparts, focusing in particular on data's mobility, divisibility, and interconnectedness. It also examines 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.

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

[11] *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 285-86 (2015) [hereinafter Kerr, *The Global Internet*].

Finally, Part III argues that these differences between data and its tangible counterparts matter, but in the exact opposite way than the government has suggested. These differences both compel a rethinking of a territorial Fourth Amendment and highlight the dangers of unilateral, extraterritorial law enforcement that data enables. More specifically, I argue that the intermingling and mobility of data means that territorial and identity-based 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 (or seizure) of data. Large quantities of protected persons' data are being incidentally collected under the much more permissive rules governing the collection of non-protected persons' information. This rules, as currently applied, are now longer providing the kind of protections to the U.S. citizens and others located within the United States that they are designed to ensure. This calls for a rethinking of the Fourth Amendment's reach,

The mobility and divisibility of data similarly expose the problems with territorially-limited warrant authority that turns on where data happens to be located at any given point in time. However, the kind of unilateral, extraterritorial exercise of law enforcement that the government advocates in the *Microsoft* case imposes its own set of costs. Among other problems, it encourages the Balkanization of the Internet into multiple, closed-off systems protected from the extraterritorial reach of foreign-based ISPs, which imposes significant costs on the efficiency and effectiveness of the Internet.[12] 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 ISP to turn over emails and other data stored in the United States, including data of U.S. citizens.[13] Thus, while this Article recognizes, and in fact embraces, the need for new norms and procedures in response to cross-border data flows, it argues that this is not something that should be unilaterally imposed. Rather, the Executive Branch should work with its foreign partners to develop improved—and agreed-upon—mechanisms for law enforcement to access data, irrespective of where it is stored.

I. TERRITORIAL PRESUMPTIONS

[12] Conversely, Microsoft's position also encourages a different form of data localization, pursuant to which nations require that their citizens' or residents' data be stored locally, thus ensuring local law enforcement access. This, too, imposes costs to the efficiency of the Internet, and, while not as costly as the creation of fully closed-off systems, is also more likely to come to fruition. *See, e.g.,* Ilya Khrennikov and Anastasia Ustinova, "Putin's Next Invasion? The Russian Web," Bloomberg BusinessWeek, 1 May 2014, available at http://www.businessweek.com/articles/2014-05-01/russia-moves-toward-china-styleinternet-censorship; Daskal, *The Microsoft Warrant Case: The Policy Issues,* Just Security, Sep. 8, 2015, https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues/ *See also infra* Part III.C.

[13] *See* Oral Argument Tr., 2d Cir. at 54-56, 58(government claiming that it is the "norm" for a German court to require a provider in Germany to turn over data wherever located, including the United States).

Increasing global interconnectedness has prompted renewed attention to the validity and effect of territorial presumptions in law. In a variety of contexts, both U.S. federal courts and the Executive Branch have sought to define and limit the geographic reach of statutes, constitutional provisions, and international treaty obligations.[14] With some notable exceptions—including the Supreme Court's ruling in *Boumediene v. Bush*[15] that the Suspension Clause extends to Guantanamo Bay detainees—the recent trend has been one of entrenchment, with territorial-based presumptions waxing, not waning. Just five years ago, the Supreme Court in *Morrison v. National Australia Bank Ltd.* upended longstanding assumptions about the reach of U.S. securities law in order to fortify the presumption against the extraterritorial application of statutory law.[16] In a unanimous opinion three years later, the Court applied the presumption to limit the extraterritorial reach of the Alien Tort Statute.[17] Meanwhile, the executive branch 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.[18] And while the Obama Administration has sought to extend certain protections to nonresident aliens in the context of foreign intelligence surveillance and targeted uses of lethal force, it has done so as a matter of *policy*, not law.[19] The law continues to depend on a

---

[14] *See infra* notes 16-18 and accompanying text; *see also* Hernandez v. United States, 785 F.3d 117 (5th Cir. 2015) (en banc) (per curiam) (applying strict, formalistic limits to the extraterritorial application of Fourth Amendment rights).

[15] 553 U.S. 723, 732 (2008) (holding that Guantanamo Bay detainees are entitled, as a matter of constitutional law, to bring habeas petitions challenging their ongoing detention).

[16] 561 U.S. 247, 255 (2010) ("When a statute gives no clear indication of an extraterritorial application, it has none.").

[17] *See* Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659 (2013). For interesting commentary, see Sarah H. Cleveland, Commentary, *The* Kiobel *Presumption and Extraterritoriality*, 52 COLUM. J. TRANSNAT'L L. 8 (2013); and 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).

[18] *See* U.S. Dep't of State, Office of the Legal Adviser, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010), http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf [https://perma.cc/BQ39-FUKH]; Charlie Savage, *U.S., Rebuffing U.N., Maintains Stance that Rights Treaty Does Not Apply Abroad*, N.Y. TIMES, Mar. 13, 2014, http://www.nytimes.com/2014/03/14/world/us-affirms-stance-that-rights-treaty-doesnt-apply-abroad.html [http://perma.cc/9WQW-2PHF]; *cf.* Press Release, The White House, Office of the Press Sec'y, Statement by NSC Spokesperson Bernadette Meehan on the U.S. Presentation to the Committee Against Torture (Nov. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-presentation-committee-a [http://perma.cc/R3XK-5MJH] (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").

[19] *See, e.g.*, Press Release, The White House, Office of the Press Sec'y, 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 [http://perma.cc/WWQ7-GAVQ]; Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities § 4 (Jan. 17, 2014),

complicated set of territorial presumptions and applications—all of which depend, at their core, on the ability to define the relevant "here" and "there" and a determination that the "here" and "there" matter.[20]

This Part sets the stage for the argument that follows. It describes key constitutional, statutory, and international law presumptions of territoriality that are embedded in the Fourth Amendment, statutory surveillance scheme, and warrant jurisdiction. As this Part highlights, the rules are based on two key premises. First, U.S. citizens and others with substantial connections to the United States are, as a matter of both constitutional law and policy, entitled to greater privacy protections than noncitizens who lack substantial connections to the United States. And second, respect for other states' sovereignty, concerns about international comity, and practical impediments to extraterritorial law enforcement actions limit the extraterritorial reach of warrants.

Notably, case law and commentary also have generally assumed—usually 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.[21]

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 criminally prosecuting its own citizens in a foreign territory.[22] Under the then-prevalent understanding of the Constitution's reach, constitutional rights had full effect within the nation's borders, but generally not elsewhere.[23] In fact, even as the United States acquired new lands, only those territories that were "incorporated"

---

http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [http://perma.cc/EN7Z-YPED] [hereinafter PPD-28].

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

[21] *See In re* Grand Jury Proceedings Bank of Nova Scotia, 740 F.2d 817 (11th Cir. 1984) (holding that a bank operating in the United States was obliged to produce financial documents located in the Cayman

Islands in response to a grand jury subpoena); *In re* Grand Jury Subpoena Directed to Marc Rich & Co., A.G., 707 F.2d 663, 667 (2d Cir. 1983) (emphasizing that "[t]he test for the production of documents [in response to a grand jury subpoena] is control, not location"; as a result, a witness may not resist production "on the ground that the documents are located abroad"); *supra* notes 1-2 and accompanying text.

[22] *See* Ross v. McIntyre, 140 U.S. 453 (1891) (holding that jury trial rights did not apply in the prosecution of a capital crime by a U.S. consul in Japan). Conversely, actions taken within the United States 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) ("The 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.").

[23] *See, e.g.*, KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG?: THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW (2009); Gerald L. Neuman, *Whose Constitution?*, 100 YALE L.J. 909, 918-19 (1991). *But see* J. Andrew Kent, *A Textual and Historical Case Against a Global Constitution*, 95 GEO. L.J. 463, 493-97 (describing select exceptions to strict territoriality prior to 1957).

within the United States (i.e., those destined for statehood) were protected by the entirety of the Bill of Rights. "Unincorporated" territories were protected by "fundamental" rights only.[24]

By 1957, the Constitution's territorial limits with respect to U.S. citizens began to crumble. After initially ruling—consistent with longstanding doctrine—that citizen-dependents of service members overseas were not entitled to Fifth and Sixth Amendment rights to a jury, the Supreme Court granted a rehearing and reversed itself the following Term.[25] Writing for a plurality in *Reid v. Covert*, Justice Black stated:

> [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.[26]

Justices Harlan and Frankfurter concurred, albeit on narrower grounds, restricting their analysis to the facts of the case; specifically, they centered their analysis on the fact that the case involved a capital murder.[27]

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 where or upon whom it was acting.[28] But in its

---

[24] Territories destined for statehood were deemed "incorporated" into the United States, whereas territories that were not slated to become states were "unincorporated" and thus "not a part of the United States." Downes v. Bidwell, 182 U.S. 244, 287 (1901); *id.* at 342 (White, J., concurring). Fundamental rights were understood at the time to include those "inherent, although unexpressed, principles which are the basis of all free government . . . restrictions of so fundamental a nature they cannot be transgressed." *Id.* at 291 (White, J., concurring). These fundamental rights were further defined to include due process rights but not "artificial or remedial" rights, such as jury-trial rights. *Id.* at 282; Balzac v. People of Porto Rico, 258 U.S. 298, 312-13 (1922) (noting that "[t]he guaranties of certain fundamental personal rights declared in the Constitution, as for instance that no person could be deprived of life, liberty or property without due process of law, had from the beginning full application" in the territories); *but see* Christina Duffy Burnett, *A Convenient Constitution? Extraterritoriality After* Boumediene, 109 COLUM. L. REV. 973, 984 (2009) (asserting that the difference between incorporated and unincorporated territories with respect to the application of constitutional rights has been overstated by courts and commentators) .

[25] *See* Kinsella v. Krueger, 351 U.S. 470 (1956); Reid v. Covert, 351 U.S 487 (1956), *reh'g granted in both cases*, 352 U.S. 901 (1956), *overruled by* Reid v. Covert, 354 U.S. 1 (1957).

[26] 354 U.S. at 5-6.

[27] *Id.* at 41-64 (Frankfurter, J., concurring); *id.* at 65-76 (Harlan, J., concurring). Three years later, Justices Harlan and Frankfurter dissented in a case that extended the jury trial protections to citizen-dependents in a non-capital case. *See* McElroy v. United States *ex rel.* Guagliardo, 361 U.S. 234 (1960) (Harlan & Frankfurter, JJ., dissenting).

[28] *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) ("The compact applies to everything done by the community and its officials, in the United States and elsewhere, affecting citizens and aliens alike, and concerning immigration no less than other matters."); 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).

1990 ruling in *United States v. Verdugo-Urquidez*,[29] the Supreme Court rejected this argument.

The *Verdugo-Urquidez* case addressed the constitutionality of a warrantless search of captured drug lord Rene Verdugo-Urquidez's residence in Mexico by U.S. agents. Verdugo-Urquidez was in U.S. custody in California at the time of the search. Both the district court and the Ninth Circuit ruled that the search violated the Fourth Amendment. But a fractured Supreme Court reversed. Justice Rehnquist—on behalf of himself and Justices White, O'Connor, and Scalia—concluded that Verdugo-Urquidez, as a non-resident alien, was not entitled to the Fourth Amendment protections. According to Justice Rehnquist, the Fourth Amendment's reference to "the people"[30] 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 this country to be considered part of that community."[31] Verdugo-Urquidez needed to have developed a "sufficient connection" to the United States in order to receive the Fourth Amendment's protection; two days in a U.S. jail could not suffice.[32] In so holding, the Court made search location and target identity the key determinants of the Fourth Amendment's reach.

Justice Kennedy provided the critical fifth vote. But while purporting to join Chief Justice Rehnquist's opinion, Justice Kennedy repudiated the majority's central theory. Specifically, he rejected the assertion that the Fourth Amendment's reference to "the people" was a term of art referring exclusively to U.S. citizens and those with sufficient connections to the United States. Justice 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."[33] However, 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

---

[29] 494 U.S. 259, 271 (1990).

[30] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

[31] *Id.* at 265. In so holding, the Court adopted what Gerald Neuman labels a "membership" theory of constitutional rights. GERALD L. NEUMAN, STRANGERS TO THE CONSTITUTION: IMMIGRANTS, BORDERS, AND FUNDAMENTAL LAW 6-7 (1996) (defining the membership theory to mean that only the "beneficiaries" of the social contract are entitled to constitutional rights protections); *see also* Chimène I. Keitner, *Rights Beyond Borders*, 36 YALE J. INT'L L. 55, 57 (2011) (defining this approach as the compact model).

[32] *Verdugo-Urquidez*, 494 U.S. at 265, 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 2015/2016).

[33] *Verdugo-Urquidez*, 494 U.S. at 276 (Kennedy, J., concurring); *see also* United States v. Verdugo-Urquidez, 856 F.2d 1214, 1223 (9th Cir. 1988) (arguing that the Framers' primary concern was to protect natural rights, thereby rejecting the attempt to "restrict[] the application of the fourth amendment to any special class of people"), *rev'd*, 494 U.S. 259 (1990).

class of noncitizens who are beyond our territory."[34] Justice Kennedy instead advocated a pragmatic approach to the extraterritorial application of constitutional rights. According to Justice Kennedy, it would be "impracticable and anomalous" to enforce the Fourth Amendment's warrant requirement in the context of a foreign search of a nonresident alien.[35] Thus, the warrantless searches of Verdugo-Urquidez's Mexican residences did not violate the Fourth Amendment.[36]

Despite the splintered analysis, *Verdugo-Urquidez* now stands for the proposition that the Fourth Amendment does not constrain the United States when its agents search or seize a noncitizen outside the United States, unless the noncitizen has developed a "significant voluntary connection" with the United States.[37] 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* subject to the Fourth Amendment, even when located extraterritorially, but that only the reasonableness test—and not the warrant requirement—applies.[38] Stated another way, government extraterritorial actions vis-à-vis U.S. citizens or other persons with sufficient connections to the United States have to be "reasonable," a standard that is generally determined by weighing the government and private interests at stake. But the government need not obtain a warrant based on a magistrate's finding of probable cause, as is the default requirement when the government searches or seizes on U.S. soil.[39]

---

[34] 494 U.S. at 275 (Kennedy, J., concurring).

[35] *Id.* at 278. This part of the opinion draws directly on Justice Harlan's concurrence in *Reid*. *See* 354 U.S. at 74-75 (Harlan, J., concurring) (arguing that the extraterritorial reach of constitutional rights should depend on practical, functional considerations, such as the "local setting, the practical necessities, and the possible alternatives"; the key test was whether "adherence to a specific guarantee [would be] altogether impracticable and anomalous").

[36] 494 U.S. at 278 (Kennedy, J., concurring). 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. Kennedy also failed to address the possibility that a warrant requirement could operate simply as a means to ensure that the requisite U.S. standards had been met (probable cause and a review by a neutral magistrate) without also providing the affirmative authorization to search or seize (which would need to be separately granted by the Mexican government).

[37] *See, e.g.*, Hernandez v. United States, 785 F.3d 117, 119-20 (5th Cir. 2015) (per curiam), *petition for cert. filed* (U.S. July 27, 2015) (15-118) (applying the "sufficient voluntary connection" standard from *Verdugo-Urquidez* finding no "sufficient voluntary connection" where the victim was an "alien who . . . was not in[] the United States when the incident occurred").

[38] *See, e.g.*, United States v. Stokes, 726 F.3d 880, 893 (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) (also applying a reasonableness test); *see also* United States v. Peterson, 812 F.2d 486, 490-91 (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 [redacted text] Pursuant to Section 105B of the 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").

[39] That said, even when the government searches or seizes a U.S. citizen on U.S. soil, there are a host of exceptions to the warrant requirement that may apply. *See Warrantless Searches and Seizures*, 44 GEO. L.J. ANN. REV. CRIM. PROC. 48 (2015) (detailing the many exceptions to the warrant requirement that apply even when the government is conducting a search or seizure on U.S. soil). For an interesting debate as to what the Fourth Amendment historically required, see Akhil Reed

Verdugo-Urquidez, thus established a two-step decision tree. First, where does the search or seizure take place? If in the United States, the Fourth Amendment applies.[40] 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 an 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 noncitizen 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.

Moreover, while the 2008 ruling in *Boumediene v. Bush*[41]—in which the Supreme Court held that the Suspension Clause protected aliens at Guantanamo Bay—precipitated new proclamations of an emergent constitutional universalism,[42] this universalism has not yet materialized. To the contrary, lower courts have largely restricted *Boumediene*'s holding to the Suspension Clause and possibly other so-called "structural" provisions of the Constitution, such as the Ex Post Facto Clause.[43] Courts continue to rely on *Verdugo-Urquidez* as a basis for concluding that

---

Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994), which argues against the presumptive warrant requirement, even as applied to the search and seizure of U.S. citizens on U.S. soil, and elucidates a theory of reasonableness; Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L REV. 547, 571-90 (1999), which critiques Amar's account of the historical record in support of a reasonableness test; and Tracey Maclin, *When the Cure for the Fourth Amendment is Worse than the Disease*, 68 S. CAL. L REV. 1 (1994), which also critiques Amar's position largely on historical, normative, and policy grounds.

[40] 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 Fourth Amendment protections. *See, e.g.*, United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1260-61, 1273 (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, 978 (4th Cir. 2012) (relying, in part, on *Verdugo-Urquidez* to conclude that illegal aliens are not entitled to Second Amendment rights). But the extension of the opinion in such a way is a minority view. Moreover, Rehnquist himself describes the holding as addressing the *extraterritorial* application of Fourth Amendment rights. *Verdugo-Urquidez*, 494 U.S. at 274 ("We think that the text of the Fourth Amendment, its history, and our cases discussing the application of the Constitution to aliens and *extraterritorially* require rejection of respondent's claim." (emphasis added)).

[41] 553 U.S. 723 (2008).

[42] *See, e.g.*, Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 230 (2010) (suggesting that *Boumediene* marked a change in U.S. jurisprudence); David D. Cole, *Rights over Borders: Transnational Constitutionalism and Guantanamo Bay*, 2007-2008 CATO SUP. CT. REV. 47, 61 (describing the Supreme Court as having rejected "outmoded claims about sovereignty, territoriality, and rights"); 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" and providing a new path of jurisprudence). 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" and stating that the Supreme Court "erred" in 2008 when the case was decided) and Eric A. Posner, Boumediene *and the Uncertain March of Judicial Cosmopolitanism*, 2007-2008 CATO SUP. CT. REV. 23, 24-25 (criticizing an emerging "judicial cosmopolitanism").

[43] *See* Al-Bahlul v. United States, 767 F.3d 1, 49 (D.C. Cir. 2014) (Rogers, J., concurring in part and dissenting in part) (noting that the Ex Post Facto Clause, like the Suspension Clause, "serves as a meaningful structural constraint imposed by Article I that goes 'to the very root of the power of

noncitizens without substantial connections to the United States lack Fourth Amendment and other so-called "individual" rights.[44] In fact, it even remains unsettled whether Guantanamo detainees are entitled to basic rights—as distinct from the Suspension Clause—protections.[45]

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" is meant to emphasize the importance of the right, rather than limit its application to a certain class.[46] David Gray, also relying on the term "the people," persuasively suggests that the term defines a collective right.[47] Relying on both textual and historical analysis, Gray argues that the term "the people" was chosen to emphasize the collective political interest in being free from unreasonable searches or seizures; "[w]henever a member of 'the people' challenges a governmental search or seizure, she therefore stands not only for herself, but for

---

Congress to act all'") (citations omitted); Brief for the United States at 80, Al-Bahlul v. United States, 767 F.3d 1 (2014) (No. 11–1324), 2013 WL 3479237, at *64 (relying in part on the Ex Post Facto's "structural function in U.S. law" as a basis for conceding that it applies to military commission prosecutions of aliens in Guantanamo); KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 244 (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."); *infra* notes 44-45.

[44] *See, e.g.*, Hernandez v. United States, 785 F.3d 117, 119 (5th Cir. 2015) (holding that an alien 15-year-old shot just over the Mexican border lacks Fourth Amendment rights given his lack of substantial connections to the United States); 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"); United States v. Emmanuel, 565 F.3d 1324, 1331-32 (11th Cir. 2009) (concluding that a non-citizen and resident of the Bahamas without substantial voluntary connections to the United States lacks Fourth Amendment rights); *see also* Ibrahim v. Dep't of Homeland Sec., 669 F.3d 983, 997 (9th Cir. 2012) (ruling that a non-citizen could raise First and Fifth Amendment claims because she had developed "significant voluntary connections" with the United States); United States v. Ali, 71 M.J. 256, 268 (C.A.A.F. 2012) (holding that an alien working as a civilian contractor in Iraq is not entitled to jury trial rights); Atamirzayeva v. United States, 524 F.3d 1320, 1329 (Fed. Cir. 2008) (concluding that an alien lacking a sufficient connection to the United States was not entitled to relief under the Takings Clause). *But see* Rodriguez v. Swartz, No. 14 Civ. 02251 (D. Ariz. July 9, 2015) (relying in significant part on the functionalist approach of *Boumediene* to conclude—in direct repudiation of the Fifth Circuit's ruling in *Hernandez*—that an alien shot just over the border in Mexico is entitled to the protections of the Fourth Amendment).

[45] *See, e.g.*, Al-Madhwani v. Obama, 642 F.3d 1071, 1077 (D.C. Cir. 2011) (asserting that "detainees [at Guantanamo Bay] possess no constitutional due process rights" (brackets in original) (citation omitted)); Rasul v. Myers, 563 F.3d 527, 529 (D.C. Cir. 2009); United States v. Hamdan, 801 F. Supp. 2d 1247, 1322 (C.M.C.R. 2011), *rev'd on other grounds*, 696 F.3d 1238 (D.C. Cir. 2012.). *But see* Brief for the United States, Al-Bahlul v. United States, 767 F.3d 1 (2014) (No. 11–1324), 2012 WL 1743629, at *82-83 (D.C. Cir. May 16, 2012) (noting that the Supreme Court has not yet decided whether Guantanamo Bay detainees are entitled to due process rights and assuming, *arguendo*, that they are in fact covered).

[46] *See supra* notes 33-35 and accompanying text.

[47] *See* David C. Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. (forthcoming 2015) (manuscript at 21), http://ssrn.com/abstract=2588739 [http://perma.cc/W35Z
-L6J7] ("[T]he Fourth Amendment should . . . be read as referring to collective rights of 'the people' rather than individual rights of each 'person' or 'subject.'").

'the people' as a whole."[48] To be sure, the import of Gray's insight depends in part on how "the people" is defined.[49] But even assuming a narrow definition of "the people" as limited to U.S. citizens and those with significant voluntary connections to the United States Gray's approach moves us away from the individualistic focus on the particular target of the government action—i.e., the idea that Jack (a hypothetical U.S. citizen) has not suffered a Fourth Amendment violation when evidence is obtained in the process of illegally searching his friend Jill. Jack, as a representative of "the people," could claim a Fourth Amendment violation any time the government's impermissible activity implicated him—regardless of whether or not he is the direct target of a search. Under such an approach, Jack could claim a Fourth Amendment violation when, in the course of targeting a non-U.S. person, the government collects Jack's communications as well. I return to this issue in Part III.

For now, it is worth emphasizing one other notable aspect of *Verdugo-Urquidez*. Specifically, *Verdugo-Urquidez* highlights the longstanding assumption that the locus of the territoriality inquiry turns on the location of the thing being searched or seized. The search of Mr. Verdugo-Urquidez's residence took place in Mexico while he was being held in the United States.[50] Throughout the case, it was simply assumed, without discussion, that the search was extraterritorial, not territorial.[51] What mattered was the location of the *property* being searched, not the location of the property's owner or the agent performing the search.

B. TERRITORIAL-BASED SURVEILLANCE AUTHORITIES

The statutory and regulatory regime governing foreign intelligence surveillance currently tracks the Fourth Amendment's focus on location and nationality as determinative of the rules that apply.[52] But this was not always the case.

Initially passed in 1978, the Foreign Intelligence Surveillance Act (FISA) regulates the collection of electronic communications for foreign intelligence purposes.[53] The 1978 version of FISA covered, among other things, the collection of wire and radio communications of persons based in the United States, as well as territorial-based acquisitions of international wire communications when the

---

[48] *Id.* at 25; *see also id.* at 22 (arguing that the term "the people" "bespeaks an understanding that security from unreasonable search and seizure is linked to collective projects of governance and politics").

[49] *See, e.g.*, Dred Scott v. Sandford, 60 U.S. (19 How.) 393, 393 n.5 (1856).

[50] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 262 (1990).

[51] *Id.* at 274-75.

[52] A quick word on terminology: The Foreign Intelligence Surveillance Act (the primary focus of this section) refers to the "acquisition" of electronic communications to describe what is colloquially understood as the "collection" of such information. I use these terms interchangeably.

[53] Pub. L. No. 95–511, 92 Stat. 1783 (codified in scattered sections of 50 U.S.C.). FISA also regulates 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.

targeted communication was to or from a person within the United States.[54] With a few narrow exceptions, all such collection required a warrant issued by the Foreign Intelligence Surveillance Court (FISC), based on a finding that the target was a "foreign power" or an "agent of a foreign power."[55]

Notably, the warrant requirement applied to citizens and noncitizens alike, albeit with heightened standards governing the targeting of a "United States person" (i.e., a U.S. citizen or legal permanent resident).[56] At the time of passage, some members of Congress argued that the warrant requirement should cover U.S. persons only—not resident aliens who were not legal permanent residents or nonresident aliens whose communications were covered by FISA when the collection took place in the United States.[57] 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."[58]

This quote exemplifies the 1978 Congress's prescient understanding of two important facts. First, the acquisition of non-U.S. persons' communications could yield the incidental collection of U.S. persons' information. The aptness of this insight has only increased over time. When Congress passed FISA in 1978, most communications were wholly domestic. In other words, communications transpired primarily between two or more U.S.-based users and involved 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 often involving at least one foreign-based sender or recipient and regularly transiting in and out of the nation's boundaries.[59] 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. persons' data.

Second, a universally applicable warrant requirement protected against erroneous citizenship determinations that would otherwise result in the warrantless surveillance of U.S. citizens. In other words, Congress demanded a warrant for the acquisition of non-U.S. persons' information not because it was interested in protecting non-U.S. persons' privacy, but as a means of protecting U.S. persons.

---

[54] *See id.* § 101 (codified at 50 U.S.C. § 1801(f)). 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 (2d ed. 2012).

[55] Foreign Intelligence Surveillance Act § 105 (codified at 50 U.S.C. § 1805(a)(2)(A)); *see also id.* § 102 (codified at 50 U.S.C. § 1802) (defining the circumstances in which the executive branch could authorize territorial electronic surveillance without a court order).

[56] *Id.* § 101 (codified at 50 U.S.C. § 1801(i)). 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.* (codified at 50 U.S.C. § 1801(i) and 8 U.S.C. § 1101); *see also id.* (codified at 50 U.S.C. § 1801(b)) (defining what it means to be an "agent of a foreign power" differently for U.S. persons and non-U.S. persons).

[57] H.R. REP. NO. 95-1283, pt. 1, at 26 (1978) [hereinafter House FISA Report].

[58] *Id.*

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

In 2008, however, Congress passed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA) and made two key changes to FISA. First, the FAA extended FISA's warrant coverage to the surveillance of U.S. persons located outside the United States, thereby bringing the extraterritorial surveillance of U.S. persons under FISA's statutory scheme.[60] Second, Congress eliminated the warrant and probable cause requirement for the domestic acquisition of electronic communicates targeted an extraterritorially-located non-U.S. person. In doing so, the 2008 Congress disregarded the insight of the 1978 Congress regarding the risk of intermingled data and erroneous targeting decisions.

In broad brushstrokes, territorial-based presumptions now operate along two axes. The first axis—the targeting of *persons* located inside the United States, as well as U.S. citizens and legal permanent residents wherever they are located (so-called "U.S. persons")—is subject to more rigorous standards and procedural protections than the targeting of noncitizens located outside the United States. The second axis—the collection of *data* located within the United States—is generally subject to heightened restrictions compared to collection that takes place outside the United States.[61] 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 FISC must approve the targeted electronic surveillance of all persons in the United States as well as all U.S. persons outside the United States, based on a finding of probable cause that the requisite targeting standard has been met. This requires finding that the target is a "foreign power," an "agent of a foreign power," or, for U.S. persons located outside the United States, an "employee or officer of a foreign power" (an addition meant to cover those working for foreign governments or foreign government-owned companies).[62]

---

[60] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (Fisa Amendments Act of 2008), Pub. L. No. 110-261, 122 Stat. 2436 (2008) §§ 703, 704 (codified at 50 U.S.C. §§ 1881b; 1881c). Protections for U.S. persons located extraterritorially were first added as an amendment to the then-pending version of the legislation in October 2007, adopted by the Senate Intelligence Committee by a fairly narrow vote of 9-6. *See* Jonathan W. Gannon, *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).

[61] The details are, of course, more complicated; not all types of electronic surveillance fits neatly into this general schema. *See, e.g.*, Jonathan Mayer, *Executive Order 12333 on American soil, and Other Tales from the FISA Frontier*, WEB POLICY (Dec. 3, 2014), http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/ [http://perma.cc/7FES-DYJM]; KRIS & WILSON, *supra* note 54, § 17:17.

[62] Rules governing the surveillance of persons in the United States (which requires a warrant based on a finding of probable cause) also vary depending on whether the target is a U.S. person or non-U.S. person. For example, the definition of "agent of a foreign power" is broader for non-U.S. persons than U.S. persons, *see* 50 U.S.C. § 1801(b) (2012); 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) (2012) (defining "foreign intelligence information" differently for U.S. persons and non-U.S. persons); and the duration of permitted acquisition is longer for non-U.S. persons, *see* 50 U.S.C. § 1805(d)(1) (2012). 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) (2012). That said, Presidential Policy Directive 28, issued January 17, 2014, stated that as a matter of *policy*, intelligence agencies

Conversely, electronic surveillance targeting non-U.S. persons located outside the United States—what is known as "702" surveillance based on the statutory provision in the FAA[63]—is now permitted without a warrant, a finding of probable cause, or even a requirement that the target be a foreign power, agent, or employee of a foreign power.[64] Rather, it is the Attorney General and the Director of National Intelligence—not the FISC—who jointly authorize the targeting of noncitizens "reasonably believed to be located outside the United States to acquire foreign intelligence information," subject to certain statutory limitations.[65]

The FISC's role is limited to three tasks. First, the FISC reviews the joint "certification" issued by the Attorney General and Director of National Intelligence to ensure it contains all the requisite elements.[66] Second, the FISC reviews whether the targeting procedures are "reasonably designed" to target those "reasonably believed" to be outside the United States and to prevent the acquisition of communications in which the sender and all recipients are U.S.-based.[67] And third, the FISC reviews minimization procedures—which are required to limit the acquisition, retention, and dissemination of information involving U.S. persons—to assess whether they contain the required elements.[68] The FISC has no role in reviewing each specific targeting decision.

In practice, a National Security Agency (NSA) analyst initiates targeting upon a determination 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 United States.[69] Because a target's identity is not always known, the NSA applies certain presumptions. For example, 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.[70] These, however, are hardly foolproof

---

must eliminate, where possible, differences in the dissemination and retention rules governing U.S. persons' and non-U.S. persons' information. *See* PPD-28, *supra* note 19, § 4.

[63] FISA Amendments Acts of 2008, Pub. L. No. 110–261 § 702, 122 Stat. 2436 (2008) (codified as amended at 50 U.S.C. § 1881(a) (2012)).

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

[65] 50 U.S.C. § 1881a(a) (2012).

[66] *Id.* § 1881a(i)(2)(A); *Id.* § 1881a(g) (describing the certification requirement). Approved certifications reportedly authorize, amongst other things, the acquisition of information concerning international terrorism and weapons of mass destruction. *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, PRIVACY & C.L. OVERSIGHT BOARD 25 & n.71 (July 2, 2014), http://www.pclob.gov/library/702-Report.pdf [http://perma.cc/V7SG-HJLZ] [hereinafter PCLOB 702 Report].

[67] 50 U.S.C. § 1881a(i)(2)(B) (2012).

[68] *Id.* § 1881a(i)(2)(C).

[69] PCLOB 702 Report, *supra* note 66, at 43-45.

[70] *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*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE § 2(k)(2) (Oct. 31, 2011), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20i

presumptions, as there are many reasons why a U.S. person might be temporarily or permanently located outside of the United States. While the Department of Justice reports that the error rate is quite low—just 0.4% in a review of 2011 data[71]—such statistics obviously only include identified errors and do not tell us anything about unknown errors. Moreover, given the sheer quantity of data that is currently being collected, even a low rate of error can yield high numbers of erroneous "foreignness" assessments.

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"[72] and effectively serves as the search term for collection and/or review of the acquired data. It is possible to have multiple selectors associated with each target.[73]

There are reportedly two main collection programs pursuant to 702: PRISM collection and upstream collection. With PRISM collection, the government sends approved selectors, such as emails associated with the targeted persons, to an electronic communications service provider, such as an ISP. The ISP must then turn over all communications sent to or from the selector to the NSA.[74] As of mid-2011, approximately ninety percent of all communications collected pursuant to 702 were obtained through PRISM—yielding an estimated 225 million Internet communications each year.[75]

---

n%20Connection%20with%20FISA%20SECT%20702.pdf [http://perma.cc/AEZ6-DFCR] [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." *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, PRIVACY & C.L. OVERSIGHT BOARD 40-41 (Mar. 19, 2014), https://www.pclob.gov/library/20140319-Transcript.pdf [https://perma.cc/P5G3-KEBW]; *see* Donohue, *supra* note 64 (describing foreignness determination under 702); PCLOB 702 Report, *supra* note 66, at 43-45.

[71] PCLOB 702 Report, *supra* note 66, at 44. These statistics do not include data obtained pursuant to Executive Order 12,333, and do not include instances in which the Department of Justice 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 (impermissibly) continued.

[72] *See* Dir. of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, NAT'S SEC. AGENCY 5 (Apr. 16, 2014), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf [https://perma.cc/28W6-AKA3].

[73] *See, e.g.*, Office of the Dir. of Nat'l Intelligence, Calendar Year 2014 Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities—Annual Statistics for Calendar Year 2014 (Apr. 22, 2015), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014 [http://perma.cc/VX5E-TFAC] (noting that a single target may be using multiple email accounts, each of which is a different selector).

[74] PCLOB 702 Report, *supra* note 66, at 7. The NSA receives all data collected through PRISM, and the CIA and FBI each receive a portion of such data. *Id.* at 34.

[75] Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *9, *25 (FISA Ct. Oct. 3, 2011) [hereinafter Bates 2011 Opinion] (referring to the fact that the NSA acquires "more than two hundred fifty million Internet communications each year pursuant to Section 702," and that approximately 91% of these communications are acquired directly from Internet Service Providers (ISPs) through the PRISM program); PCLOB 702 Report, *supra* note 66, at 33-34; The Intelligence Community's Collection Programs Under Title VII of the Foreign

Upstream collection, by contrast, involves the acquisition of data from the so-called Internet "backbone"—the fiber-optic cables over which Internet communications travel.[76] Whereas collection through the PRISM program is done with the assistance of the ISP or phone service providers with whom the target interacts, "upstream" collection is done with the assistance of the Internet and telecommunications companies that control the fiber-optic cables over which a target's communications travel. As with PRISM, the government sends a list of approved selectors to the relevant companies. Because of the way the technology operates, acquisition generally involves the gathering up of so-called Internet "transactions." Such transactions are sometimes comprised of individual discrete communications and sometimes include multiple communications bundled together.[77] Transactions are first screened to eliminate what are known as "wholly domestic communications," defined to include transactions in which the sender and all recipients are located within the United States.[78] Then, the transactions are screened to determine whether they contain the tasked selector.[79]

There are three points worth noting about upstream collection. First, as just described, the screening requires the NSA to eliminate only those communications in which the sender and recipients are "known" to be located in the United States. However, in many cases the location of the sender and recipient are unknown. Moreover, even if the filtering tools employed by the NSA operate with 100% accuracy, the prohibition on the acquisition of domestic communications is quite narrow. It is limited to those communications in which the sender and *all* recipients are located in the United States at the time of the communication. It would not include an email update sent to thirty friends and family members, so long as one of the thirty recipients was outside the United States at the time he or she received the communication.

Second, such collection does not just yield information that is "to" or "from" a tasked selector. Rather, the entire transaction (not just the to/from line) is screened to determine whether it contains the approved selector. This yields communications that are "about" a selector—i.e., communications in which the target is referenced, but is neither the sender nor the recipient of the communications.[80] Thus, even though 702 collection is directed at non-U.S. persons located outside the United States, the NSA can collect a U.S. person-to-U.S. person communication as long as the communication is "about" (or mentions) the tasked selector.

Intelligence Surveillance Act, at 4 (2012), http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [http://perma.cc/FKN6-LMYN] (asserting that in June 2011 upstream collection accounted for "only about 11% of the overall section 702 volume").

[76] PCLOB 702 Report, *supra* note 66, at 8; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra* note 75, at 3-4 (2012).

[77] Bates 2011 Opinion, *supra* note 75, at *5.

[78] *See* 50 U.S.C. § 1881a(b)(4) (prohibiting the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States"); PCLOB 702 Report, *supra* note 66, at 37-38.

[79] PCLOB 702 Report, *supra* note 66, at 37.

[80] Bates 2011 Opinion, *supra* note 75, at *5; PCLOB 702 Report, *supra* note 66, at 37-38.

Third, as of 2011, approximately ten percent of the 26.5 million Internet transactions acquired annually via upstream collection involved the acquisition of what are known as "multiple communication transactions." These are multiple discrete communications packaged together for the purpose of transiting the fiber-optic lines.[81] As long as one of the discrete communications included in the transaction contains information "to," "from," or "about" the tasked selector, the NSA acquires the entire multi-communication transaction, including other discrete communications that may not contain the selector.[82] According to one analysis, the acquisition of multiple communication transactions resulted in the collection of tens of thousands of communications each year that were not "to," "from," or "about" the tasked selector, yet nonetheless acquired.[83] Acquisition of multi-communication transactions also resulted in the gathering up of tens of thousands of wholly domestic communications.[84] As Judge Bates, then-Chief Judge of the FISC, wrote in 2011, the "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."[85]

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 Executive Order 12,333 accounts for an even greater share of electronic surveillance activities than any equivalent surveillance conducted under FISA or FAA.[86]

Executive Order 12,333 prohibits the warrantless targeting of U.S. persons' communications in situations where a warrant would have been required had law enforcement agents in the United States been conducting the search.[87] Yet reports indicate that large quantities of U.S. persons' information is being obtained

---

[81] Bates 2011 Opinion, *supra* note 75, at n.32 & *26.

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

[83] *See* Bates 2011 Opinion, *supra* note 75, at *14 ("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."); PCLOB 702 Report, *supra* note 66, at 40;. *But see* Bates 2011 Opinion, *supra* note 75 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").

[84] Bates 2011 Opinion, *supra* note 75, at *11 & n.32 (describing an estimated 2,000 to 10,000 multiple communication transactions that include at least one wholly domestic communication, plus an estimated 46,000 single communication transactions that were not screened out as wholly domestic—for example, when 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).

[85] *See id.* at *25-26 (emphasizing that the tens of thousands of non-target, protected communications collected annually is a "*very* large number" (emphasis in original)).

[86] *See*, *e.g.*, Alvaro Badoyo, *Executive Order 12333 and the Golden Number*, JUST SECURITY (Oct. 9, 2014, 10:14 AM), http://justsecurity.org/16157/executive-order-12333-golden-number/ [http://perma.cc/Q8ZH-NM6G]; 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 [http://perma.cc/6DHP-TNES].

[87] *See* 50 U.S.C. § 1881c(a)(2); *see also* Gannon, *supra* note 60, at 89.

pursuant to surveillance governed by Executive Order 12,333.[88] Of note, such collection reportedly includes "vacuum cleaner" or "bulk" collection, pursuant to which the executive sweeps in all communications that transit a particular cable without using a selector or other search term to limit the scope of the acquired data.[89] Reports suggest that bulk collection has included, among other things, Internet metadata;[90] webcam chats;[91] cellphone location data;[92] and email address books.[93] 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 based on a largely unreviewable executive branch determination that such collection would not require a warrant if done for law enforcement purposes in the United States.[94]

In short, while FISA putatively requires a warrant for the collection of U.S. persons' information, in practice such information can be collected without a warrant in one of six situations: (1) if the 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 U.S. person is party to those communications; (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; (5) when the government, pursuant to Executive Order 12,333, engages in "vacuum cleaner" collection and therefore is not technically "targeting" any one person in particular;

---

[88] *See* Tye, *supra* note 86.

[89] *See* PPD-28, *supra* note 19, § 2 (referencing signals intelligence collected in "bulk" and defining "bulk" collection to mean "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)" for specified purposes).

[90] *See* Tye, *supra* note 86.

[91] Spencer Ackernman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, GUARDIAN, Feb. 28, 2014, http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam -images-internet-yahoo [http://perma.cc/KN9D-76HM].

[92] *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST, Dec. 3, 2013, http://www.washingtonpost.com/world/national -security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04 /5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [http://perma.cc/8TB2-69CA]. Though the NSA denies that it is "intentionally collecting bulk cellphone location information about cellphones in the United States," such bulk collection of cell phone location information outside the U.S. inevitably sweeps in millions of U.S. mobile phone users who travel abroad every year. *Id.*

[93] *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_story.html [http://perma.cc/FS9J-2LKY].

[94] *See* 50 U.S.C. § 1881c(a)(2) (2012) ("No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances *in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes* [without a FISC-approved order or an Attorney General-issued emergency exception] . . . ." (emphasis added)).

or (6) when collection occurs 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 restrictions on the targeting of U.S. persons. 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 scheme governing foreign intelligence surveillance is premised on an assumption that persons located in the United States are entitled to greater privacy protections than those outside U.S. borders, and that U.S. persons are entitled to greater privacy protections than non-U.S. persons. Yet, given the scope of incidental collection, the current system provides only marginal protections for the U.S. persons it is designed to protect.

In response to these concerns, the intelligence community points to minimization rules that limit the retention, dissemination, and access to collected U.S. persons' data.[95] And minimization rules, if sufficiently robust, can provide important privacy protections. But it is worth noting that Congress to date has given only scant attention to minimization rules and other use restrictions. While Congress has mandated the implementation of minimization procedures, it has delegated all the key details to the executive branch.[96] Meanwhile, it has made acquisition of data its central focus, legislating extensively on both the substantive standards and procedural requirements governing the acquisition of electronic data. Congress thus appears to be operating under the assumption that the collection itself constitutes a privacy intrusion—and thus a potential harm—that needs to be regulated.[97] To the extent that Congress, the public, and the courts remain

---

[95] *See, e.g.*, 50 U.S.C. § 1801(h) (2012) (defining minimization procedures); 50 U.S.C. § 1802(a)(2) (2012) (requiring compliance with the minimization procedures adopted by the Attorney General); Office of the Dir. of Nat'l 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 [http://perma.cc/J69Q-6MKA] (emphasizing the importance of limitations on the use, dissemination, and retention of collected data); *see also* David Cole & Marty Lederman, *Data Mining, Section 215, and Regulating the Government's* Use *of Stored Data: The Overlooked, but More Important, Question About NSA Surveillance*, JUST SECURITY (Dec. 23, 2013), http://justsecurity.org/4932/review-group-intelligence -communications-technologies-bulk-data-collection-section-215 [http://perma.cc/L5F3-CHNQ] (emphasizing the often overlooked importance of the "use" question).

[96] *See, e.g.*, 50 U.S.C. § 1881a(e) (delegating to the Attorney General, in consultation with the Director of National Intelligence, the responsibility of adopting the specific minimization procedures that meet the overarching statutory requirements).

[97] There is a rich and thick literature articulating the privacy harm that flows from collection. I do not purport to identify the primary concerns for Congress (which I suspect are multiple and varied) or rank the relevant theories of harm. Rather, I just note the variety of possible harms, ranging from the impact on personal autonomy and dignity to more consequentialist harms about how the information might be used in the future to chill speech or to shift the balance of power between the government and the governed. *See, e.g.*, 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"); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487-88 (2006) (describing privacy as, among other things, protecting against "architectural" harms—information gathering that creates a risk of future harm or that shifts the balance of power

concerned about—and therefore seek to limit—the government's acquisition of U.S. persons' data, the current set of territorial and identity-based distinctions fail to serve these goals. I return to this issue in Part III.

C. TERRITORIAL WARRANT AUTHORITY

The warrant authority's territorial-based limits implicate a very different set of considerations than those underlying the Fourth Amendment and rules on foreign intelligence. Whereas the limitations on the Fourth Amendment's reach reflect the government's assessment of who is entitled to privacy protections vis-à-vis the U.S. government, the limits on the warrant requirement stem largely from respect for state sovereignty and an array of pragmatic and related policy concerns. The overarching rule is that the judiciary's warrant authority is territorially limited.[98] After all, under well-accepted principles of international law, State *A* can exercise law enforcement actions in State *B* only if State *B* consents.[99] As a result, judges are presumed to lack authority to unilaterally authorize extraterritorial searches and seizures.[100]

The following describes these territorial limits as applied to "ordinary" warrants issued pursuant to the Federal Rules of Criminal Procedure (Rule 41),[101] warrants issued under the Wiretap Act (authorizing real-time collection of electronic communications),[102] and warrants issued under the Stored Communications Act (authorizing collection of stored communications).[103] 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 accessing the data? As described below, the answer is unclear, and the government has suggested different answers depending on the context and its preferred outcome.

---

between the government and the governed and results in a chilling effect); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 8-9, 14-77 (2008) (cataloguing the varied conceptions and limitations of privacy in a variety of contexts).

[98] *See infra* Parts II.A.1-3.

[99] *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW IN THE UNITED STATES § 432(2) (AM. LAW INST. 1987) ("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."); JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 478-79 (8th ed. 2012); Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 372 (2009) ("The exercise of enforcement jurisdiction in the territory of another state, without its consent, breaches the non-intervention principle . . . . [E]xtraterritorial enforcement measures will nearly always be considered illegal.").

[100] *See, e.g.*, *In re* Terrorist Bombings of U.S. Embassies in E. Afr. (Fourth Amendment Challenges) (*Odeh*) 552 F.3d 157, 169 (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.").

[101] FED. R. CRIM. P. 41.

[102] 18 U.S.C. §§ 2510-2522 (2012).

[103] 18 U.S.C. §§ 2701–2712 (2012).

1. Rule 41

Rule 41 of the Federal Rules of Criminal Procedure prescribes the authority of magistrate judges to issue a warrant for a search or seizure.[104] 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 still widely understood to be subject to territorial-based limitations.[105] In fact, the only instances in which magistrate judges are explicitly authorized to issue a warrant with extraterritorial reach are limited to situations in which: (1) the property or person to be searched or seized is located in a U.S. territory, possession, or commonwealth; (2) the object of the search is on the premises of a U.S. consular or diplomatic mission; or (3) the object of a search is on a residence or land owned or leased by the United States and used by U.S. diplomats or consular officers.[106] All three exceptions extend to locations where the United States already exerts significant (if not exclusive) regulatory authority, thereby avoiding potential conflicts with foreign jurisdictions and maintaining respect for other nations' 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.[107]

A recently proposed amendment to Rule 41 has again raised questions about the territorial limits of the judiciary's warrant authority.[108] The amendment—proposed by the Department of Justice (DOJ)—would authorize judges to issue remote access search warrants for electronically stored data in situations where the location of the device or stored data being investigated is unknown.[109] Notably, DOJ 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

---

[104] FED. R. CRIM. P. 41.

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

[106] FED. R. CRIM. P 41(b)(5).

[107] *See* Amendments to the Federal Rules of Criminal Procedure*,* 129 Fed. R. Dec. 559 (1990) ("The Court is of the view that the [proposed amendment to Rule 41 allowing for the issuance of search warrants with extraterritorial effect] requires further consideration."); *id.* at 573, 577 (describing and providing text of the proposed amendment).

[108] *See Proposed Amendment to Rule 41*, ADVISORY COMM. ON CRIMINAL RULES 165, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda Books/Criminal/CR2014-04.pdf [http://perma.cc/5ZQ5-NC6H]. The public's comments on the proposal were due on February 17, 2015. The amendment will become effective on December 1, 2016 if approved by the relevant authorities (the Advisory Committee, the Committee on Rules of Practice and Procedure, the Judicial Conference, and the Supreme Court) and if Congress does not act to defer, modify, or reject it.

[109] *See* Raman Letter, *supra* note 9, 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"); *see also* Timberg & Nakashima, *supra* note 9 (describing use of remote search tools in a terrorism case).

accessing the data would be within the magistrate's district. But at least one magistrate judge rejected the government's request.[110] In his 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."[111] The magistrate thus defined the relevant locus of the search and seizure as that of the computer or data being gathered, rather than the location of the agents accessing the device. Since the location of the computer was unknown, the magistrate lacked jurisdiction to issue the warrant.[112]

The Department of Justice responded to the magistrate judge's ruling with its proposed rule revision—arguing that the authority is needed to address situations in which anonymization tools disguise the location of a computer or other device being used for criminal activity.[113] But while the proposed rule responds to the problem of anonymization, it raises the prospect of judges authorizing what could turn out to be extraterritorial searches. After all, if the location of the target device and/or data is unknown, agents and reviewing judges will not know whether the sought-after data is located territorially or extraterritorially. In fact, data on Tor (one of the largest anonymity networks[114]), indicates that more than eighty percent of its users connect to the network from *outside* the United States. [115] This suggests a likelihood that DOJ would be conducing extraterritorial searches in precisely the situations that are motivating

---

110 *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 761 (S.D. Tex. 2013).

111 *Id.* at 757. This argument has obvious parallels to the Supreme Court's concern in *Riley v. California*, 134 S. Ct. 2473 (2014), in which the Supreme Court ruled that the warrantless search of a cell phone incident to arrest violated the Fourth Amendment. *Id.* at 2495. 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." *Id.* at 2491.

112 *In re Warrant to Search a Target Computer*, 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).").

113 *See* Raman Letter, *supra* note 9, at 2 (emphasizing that circumstances "where investigators can identify the target computer, but not the district in which it is located—[are] occurring with greater frequency in recent years").

114 Tor describes itself as a "free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security." *Tor Project*, TOR, https://www.torproject.org [https://perma.cc/WC5T-GUSY] (last visited Aug. 28, 2015, 3:33pm). Anonymity networks operate by allowing users to access the Internet while hiding their identity by, for example, hiding the identity of the device being used to access the Internet and thereby concealing sites accessed. *See* Patrick Howell O'Neill, *Tor and the Rise of Anonymity Networks*, THE DAILY DOT, Oct. 24, 2013, http://www.dailydot.com/technology/tor-freenet-i2p-anonymous-network [http://perma.cc/XYG9-KSB9].

115 *See TOR Metrics—Top-10 Countries by connecting Users*, TOR PROJECT, https://metrics.torproject.org/userstats-relay-table.html [https://perma.cc/4UQX-SME5] (estimating that only about 18% of Tor's daily users are based in the United States); *see also* Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (Sept. 14, 2014, 9:10 AM), http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/ [http://perma.cc/ET34-PD3C] (raising concerns about the ways in which this amendment will lead to extraterritorial searches and seizures).

the proposes amendment—situations in which the device location has been concealed through the use of anonymity tools.Moreover, even when a targeted device is located territorially, the data accessed from the device may be stored extraterritorially.

In a letter to the Rules Committee, Mythili Raman, the Criminal Division's Acting Assistant Attorney General, responds to the possibility of such extraterritorial searching: "[S]hould the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search."[116] In other words, DOJ concedes that warrants issued under its proposed rule change would not have extraterritorial reach; after all, judges have no statutory authority to issue warrants with extraterritorial effect. But this raises a series of significant yet unanswered questions about what agents will be instructed to do if and when they discover that they are engaged in an extraterritorial search. For example, 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 judge has warned that he might not be able to issue a warrant even with the rule change, given the risk that he might be issuing an extraterritorial warrant.[117]

The government's position with respect to this proposed rule revision is notable for at least two additional reasons. First, DOJ appears to accept, contrary to its position at least on earlier search warrant applications,[118] that the relevant search or seizure occurs where the data is located, and not where the government accesses it. After all, Raman's letter explicitly asserts: "In light of the presumption against international 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."[119] Here, the government is assessing territoriality based on the location of the *data*, not the agents accessing data who presumably remain in the United States.

Second, the proposed amendment 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 that computer could be used 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.[120] Yet, according to the government's submission, if the

---

[116] Raman Letter, *supra* note 9, at 5.

[117] Conversation with the Hon. Stephen Wm. Smith, U.S. Magistrate Judge, S. Dist. of Tex. (June 5, 2015).

[118] *See In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013) ("Under the Government's theory, because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes 'property located within the district.'").

[119] Raman Letter, *supra* note 9, at 4.

[120] *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (noting that a cell phone can be "used to access data located elsewhere, at the tap of a screen"); Eric Griffith, *What Is Cloud Computing?*, PC MAG. (Apr. 17, 2015), http://www.pcmag.com/article2/0,2817,2372163,00.asp [http://perma.cc/H474-MZWJ] (explaining that with cloud computing one stores and accesses data over the Internet, rather than on one's own hard drive).

government *knew* the data was being held in Ireland (as it does in the *Microsoft* case) the magistrate could *not* issue the warrant. The government's position with respect to the proposed amendment is thus in tension with its stance in the *Microsoft* case. In the *Microsoft* case, the government is arguing that the location of the data is irrelevant when it compels a third party to produce the requested data.[121] But here, DOJ concedes that the location of the data matters if it is the *government* doing the searching or seizing.

2. Wiretap Authority

The Wiretap Act, first codified in 1968, covers real-time interception of wire, oral, or electronic communications.[122] Every court to consider the issue has concluded that the Wiretap Act only governs interceptions that occur within the territory of the United States—a conclusion that is supported by the presumption against the extraterritorial application of statutes, the legislative history of the Act, and the territorial limits on magistrate judges' warrant jurisdiction found in Rule 41.[123] However, all of these cases deal with instances in which both the agents accessing the data and the data being accessed were outside the United States.[124] The courts have not yet, as far as I know, addressed a situation in which an interception order is issued for a device that is located or travels outside the United States, but is being tapped by agents located within the United States.

An analogous issue has arisen, however, with respect to 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

---

[121] *See infra* Part II.C.

[122] 18 U.S.C. §§ 2510-2522 (2012). 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 non-relevant 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.").

[123] *See, e.g.*, United States v. Peterson, 812 F.2d 486, 492 (9th Cir. 1987) (rejecting the argument that the wiretapping of telephones in Thailand could violate the Wiretap Act); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978) (holding that the Wiretap Act did not apply to an 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 authorizations for a wiretap in a foreign country."); United States v. Angulo-Hurtado, 165 F. Supp. 2d 1363, 1369 (N.D. Ga. 2001) (concluding that the Wiretap Act does not have an extraterritorial effect); *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").

[124] In *United States v. Cotrini*, 527 F.2d 708, 711 (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 Stowe*, 588 F.2d at 341 n.12 ("That [the defendant] was in the United States when his calls were intercepted does not change the result here. The law of the locality in which the tap exists (and where the interception takes place) governs its validity, even though the intercepted phone conversations traveled in part over the United States communication system."(citing *Cotrini*, 527 F.2d at 711)).

Wiretap Act cases have suggested that 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—which permits judges to authorize the "interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting"[125]—numerous district and circuit courts have looked to both the locus of the device being tracked and the locus of the agents as a basis for establishing jurisdiction.[126] In other words, so long as *either* the agents listening in on the conversations *or* the device or wires being tapped are within the judge's district, then the jurisdiction requirement (territoriality) is satisfied.

But the issue is not settled. At least one circuit court has disagreed, concluding that the physical listening device must be installed within the authorizing court's district, even if a device installed elsewhere will be monitored by agents operating within the district.[127] Thus, at least in the D.C. Circuit, the location of the property being tracked—not the location of the agents—controls.[128] Moreover, all the cases involve situations in which both the agents and the device being monitored are located within the United States, leaving unresolved the rule that applies if the agent is located territorially but the device being monitored is located outside the United States.

3. The Stored Communications Act

A separate statutory scheme—the Stored Communications Act (SCA)[129]—governs the collection of stored data, such as emails housed on a server or documents stored in the cloud. Passed in 1986 as part of the Electronic Communications Privacy Act (ECPA), the SCA criminalizes unauthorized access to, and disclosure of, stored communications. It lays out the procedures and standards by which law enforcement agents can lawfully compel disclosure from an ISP, and is the statute at issue in the *Microsoft* case.[130] It specifies different forms of compulsory processes—subpoena, court order, and warrant—that vary in terms of what they require and when they apply.[131]

---

[125] 18 U.S.C. § 2518(3) (2012).

[126] *See, e.g*, United States v. Luong, 471 F.3d 1107, 1109 (9th Cir. 2006) ("The 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); United States v. Denman*,* 100 F.3d 399, 403 (5th Cir. 1996); United States v. Rodriguez*,* 968 F.2d 130, 136 (2d Cir. 1992), *cert. denied*, 506 U.S. 847 (1992).

[127] United States v. Glover, 736 F.3d 509, 514-15 (D.C. Cir. 2013) (finding a Title III warrant invalid because the mobile interception device was installed on property located outside the authorizing judge's jurisdiction).

[128] *Id.*

[129] 18 U.S.C. §§ 2701-2712 (2012).

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

[131] 18 U.S.C. § 2703 (2012).

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.[132] When proceeding by subpoena, the government must either notify the customer, thus providing an opportunity to object, or obtain a delayed notification order.[133] Delayed notification is permitted based on a court-approved "adverse result" finding, defined to include, among other things, destruction or tampering with evidence, flight from prosecution, endangerment of individuals, or undue trial delay.[134]

A court order is required to obtain more detailed records about a customer's activities, such as historical logs detailing the email addresses with which the customer has communicated, records of what IP addresses the user visited over time, and buddy lists.[135] A magistrate judge issues a court order based on a finding of "specific and articulable facts" that the information sought is "relevant" to an ongoing criminal investigation.[136]

Finally, in order to compel an electronic service provider to disclose the content of communications (i.e., emails) stored for 180 days or less, the government must obtain a warrant based upon a finding of probable cause.[137] Several courts have concluded that, as a matter of constitutional law, the warrant requirement also applies to the acquisition of all emails, including those stored for more than 180 days, as well as emails held by remote storage providers, which are not covered by the statutory warrant requirement.[138]

---

[132] 18 U.S.C. § 2703(c)(2) (2012).

[133] 18 U.S.C. §§ 2703(b), 2705 (2012) (describing delayed notification standards and procedures).

[134] 18 U.S.C. § 2705(2) (2012).

[135] 18 U.S.C. §§ 2703(c)(1)(E), 2703(c)(2) (2012).

[136]18 U.S.C. § 2703(d) (2012) (detailing requirements of a court order).

[137]18 U.S.C. § 2703(a) (2012). At the time the SCA was passed, the category of emails stored for 180 days of less 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).

[138] *See* Kerr, *The Next Generation*, *supra* note 10, at 383 (describing evolution of different rules for so-called "electronic communications service" providers and "remote computing service" providers). Only stored emails of electronic service providers are protected by a warrant requirement under the statute, *see* 18 U.S.C. § 2703(a) (2012); emails and other content held by remote service providers can be disclosed pursuant to a court order or even administrative subpoena, *see id.* § 2703(b). *But see* 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 Case Nos. 12-MJ-8119-DJW & Info. Associated with 12-MJ-8191-DJW Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider."); United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (citing *Warshak* for the proposition that "individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider"); *see also* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (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 provider's server). That said, the government continues to argue in the *Microsoft* case that *Warshak* got it

The legislative history, coupled with the presumption against extraterritoriality, overwhelmingly supports the conclusion that the SCA does not apply extraterritorially. 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."[139] When Congress amended the statute in 2001 to authorize magistrates to issue multidistrict warrants, the amendment was entitled "*Nationwide* Service of Search Warrants for Electronic Evidence."[140] Unsurprisingly, the one case (other than the *Microsoft* case) to present the question of the SCA's geographic reach concluded that it was territorially limited. In *Zheng v. Yahoo! Inc.*, a district court judge rejected the plaintiff's argument that the SCA applied to the conduct of Yahoo! China.[141] 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.[142] The key question, therefore, was whether Yahoo!'s United States headquarters 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.

As with the Wiretap Act, it is clear that a territorial presumption applies to the SCA. But the question of *how* this presumption applies when an international border separates the data and the person or entity accessing the data remains unsettled. What is the relevant location for determining territoriality—that of the ISP accessing the data or that of the data itself? In the *Microsoft* case, the government is arguing that it is the location of the ISP that controls. In making this claim, the government makes two analytical moves: First, the government emphasizes the language of compulsory process. The SCA authorizes the use of a warrant to "require . . . disclosure"—employing language of required disclosure that generally applies to subpoena power. According to the government, the subpoena power thus provides the appropriate frame of reference.[143] Second, the government draws on rules governing subpoenas, which require the recipient of the subpoena to turn over information within its control, irrespective of its location. What matters, according to the government, is the location of the ISP (the recipient of the warrant)—not the location of the data.[144]

But, as Microsoft and several amici have noted, there are two flaws with this argument. First, Congress used the term "warrant" in the SCA, not subpoena; there is thus good reason to think that the rules governing warrants—not

---

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 actually opened and reviewed by government agents. *See* Oral Argument Tr., Dist. Ct., *Microsoft*, *supra* note 1, at 4.

139 H.R. REP. NO. 99-647, at 32-33 (1986).

140 Uniting and Strengthening America 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 (emphasis added); H.R. REP. NO. 107- 236, at 57 (2001).

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

142 *Id.* at *1, *4.

143 *See* 18 U.S.C. § 2703(a) (2012); Appellee Brief, *Microsoft*, *supra* note 1, at 17-18.

144 Appellee Brief, *Microsoft*, *supra* note 1, at 9 ("Under long settled precedent, the power of compelled disclosure reaches records stored abroad so long as there is personal jurisdiction over the custodian and the custodian has control over the records."); *id.* at 26-30.

subpoenas—control.[145] Second, even if the analogy to subpoenas is the correct one, subpoenas generally have been relied upon to compel disclosure of a company's *own records*; they have not traditionally been relied upon to compel disclosure of a *customer's* private data that has been stored with the company.[146] The government could not, for example, use a subpoena to compel a post office to turn over mail it is transporting. Nor could the government use a subpoena to compel a landlord to collect and turn over the papers stored in a tenant's home. This is for good reason. One ought to maintain a reasonable expectation of privacy in property that is being entrusted with a third party for the limited purposes of transmittal or storage.[147]

I return to these issues in Part III.C. For now, it is simply worth noting that while the SCA is rightly understood to be territorially limited, 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 SCA's drafters, who wrote at a time when the Internet was still in its infancy and few communications crossed international borders.[148] And none of the subsequent amendments to the SCA addressed 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.

---

[145] *See* Brief for Appellant at 16, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 8. 2014) [hereinafter Appellant Brief, *Microsoft*] ("There is no basis in the statute's text for the district court's conclusion that Congress actually meant to create a new 'hybrid' subpoena when it said warrant."); Brief of Amici Curiae Amazon.com, Inc. and Accenture PLC in Support of Appellant at 5-8, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) [hereinafter Amazon Amici, *Microsoft*] (emphasizing key differences between warrants and subpoenas); Brief of Amici Curiae Media Organizations in Support of Appellant at 17-27, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014).

[146] *See* Appellant Brief, *Microsoft*, *supra* note 145, at 16-17 ("[A] bank can be compelled to produce the transaction records from a foreign branch, but not the contents of a customer's safe deposit box kept there."); Brief for Amici Curiae Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation in Support of Appellant at 17-18, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) (arguing that while subpoenas my be sufficient to obtain business records, they are not sufficient for obtaining a customer's emails); Brief of Verizon Communications Inc., Cisco Systems, Inc., Hewlett-Packard Co., Ebay Inc., Salesforce.com, Inc. and Infor, as Amici Curiae in Support or Appellant at 20, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) (emphasizing that "the *Bank of Nova Scotia* doctrine has never been extended beyond a company's own business records to reach information belonging to a company's customers"). *But see* Appellee Br. *Microsoft, supra* note 1, at 37-39 (rejecting proposition that the subpoena authority is limited to the acquisition of a corporation's business records and citing cases); Oral Argument Tr., 2d Cir, *Microsoft,* at 47-49 (same).

[147] *See* Kiel Robert Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. (forthcoming 2016) (laying out the normative justification for such a rule); *infra* note 189 and accompanying text.

[148] *See* Kerr, *The Next Generation*, *supra* note 10, at 405 ("[I]ssues regarding the territorial scope of the statute did not arise in early debates over ECPA. Congress was instead focused on the rights of U.S. computer users and U.S. services.").

* * *

To recap, 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 determinative of the rules that apply. However, territoriality serves different underlying purposes in the different constitutional and statutory contexts 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. persons 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 who lacks substantial connections to the nation and is located outside the United States.

The nation's foreign intelligence surveillance scheme adopts this basic approach as well. Targeting of U.S. persons and persons located within the United States is subject to heightened procedural and substantive protections as compared with non-U.S. persons located outside the U.S. boundaries. Similarly, collection of data physically located in the United States is 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 for the political and diplomatic consequences of failing to do so. The unilateral exercise of law enforcement in another state's territory is a breach of that state's sovereignty, potentially justifying countermeasures under international law.[149] While there may be times when law enforcement or national security interests override international law considerations, this is generally a decision best made by the political branches after a full analysis of the costs and benefits—not hundreds of federal and state court judges scattered across the country.[150] Territorial limits on warrant jurisdiction reflect this basic understanding.

But, as the following Part highlights, data is beginning to challenge these established understandings.

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.

---

[149] *See, e.g.*, Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700-07 (defining countermeasures and explaining their potential applicability in response to breaches of sovereignty).

[150] *See* 18 U.S.C. § 2703(c)(1)(A) (2012) (authorizing federal magistrates, federal judges, and state court judges to issue ECPA warrants pursuant to the requisite procedures); *About Us*, FED. MAGISTRATE JUDGES ASSOC., http://www.fmja.org/about-us.html [http://perma.cc/B6WR-RU98] (stating that there were 527 full-time magistrate judges in 2011).

This Part explores how data differs from its tangible counterparts and why these differences matter. It focuses in particular on data's mobility, divisibility, location independence, intermingling, and third party control.

A. DATA'S MOBILITY

Physical objects moving from place to place are constrained by the ordinary laws of physics and by generally observable and conscious choices about how to move from Point A to Point B. For example, a person traveling from Washington, D.C. to Philadelphia will generally take the most direct route by traversing across Maryland and Delaware. If the traveler detours to France, it is likely the result of a planned decision. The same is true for data's closest tangible counterpart—mail. It is highly unlikely that either the United States Postal Service would send a letter through Paris on the way from Washington, D.C. to Philadelphia absent some significant snafu. Similarly, when one stores tangible property in a safe-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. 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 to show up on the recipient's computer screen.[151] 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 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 safe-deposit box. It may be moved around for technical processing or server maintenance reasons. It could also be copied or divided up into component parts and stored in multiple places—some territorially and some extraterritorially.[152] At any given moment, the user may have

---

[151] *See, e.g.*, *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2006) (statement of General Michael V. Hayden, Dir., Cent. Intelligence Agency), http://www.judiciary.senate.gov/imo/media/doc/hayden_testimony_07_26_06.pdf [http://perma.cc/7GRJ-FA7C] ("A single communication can transit the world even if the communicants are only a few miles apart.").

[152] *See, e.g.*, Oral Argument Tr., Dist. Ct., *Microsoft*, *supra* note 1, at 20 ("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*, FBI L. ENFORCEMENT BULL. (Oct. 7, 2014), https://leb.fbi.gov/2014/october/executing-search-warrants-in
-the-cloud [http://perma.cc/K2N5-U5MF] ("[I]n a cloud-computing environment . . . little, if any, data pertaining to a computer user is found in a single geographic location."); *Data Centers*, GOOGLE, http://www.google.com/about/datacenters/inside/data-security/index.html [http://perma.cc/6Z2V-KKQR] (detailing Google's data storage across multiple servers in various locations). *But see* Brief for Amici Curiae Computer and Data Science Experts in Support of Appellant Microsoft Corp. at 21, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) [hereinafter Brief for

no idea—and no ability to know—where his or her data is being stored or moved, 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 circuitous and arbitrary ways, all at breakneck speed. 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.[153] 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 that data travels is often determined without the knowledge, choice, or even input of the data user.[154] 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 that sovereign nation's laws. 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 individual 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 the Fourth Amendment or statutory protections governing the 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; these are decisions that are instead entrusted to computer algorithms. The user thus lacks knowledge and choice as to the rules that apply.[155]

Computer and Data Science Experts, *Microsoft*] ("[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.").

[153] Appellee Brief, *Microsoft*, *supra* note 1, 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 (i.e., the delay between the time the data is requested and the time it is delivered). *See In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014) (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, *Microsoft*, *supra* note 152, at 20 (noting that Google seeks to keep data near its Gmail users).

[154] *See, e.g.*, Cauthen, *supra* note 152 ("The problem is that finding where . . . data is physically stored can be very difficult—even the user might not know where it is.").

[155] This lack of knowledge or conscious choice can be addressed through the introduction of term of service agreements that specify the location of one's data. A number of governments are also considering legislation that would require certain data be stored domestically. *See, e.g.*, Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (surveying localization laws).

B. DATA'S DIVISIBILITY AND DATA PARTITIONING

Data stored in the cloud is often copied and held in more than one location. This protects against server malfunctions and ensures 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.[156] This is akin to making multiple copies of one's documents and storing those copies in multiple jurisdictions. This practice, therefore, is not 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 possibly multi-nation—storage.

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.[157] The various components of a partitioned database may be held in multiple locations. In certain instances, so-called "relational databases" are only comprehensible if pulled up using the appropriate application. A health care provider, for example, may be able to pull up a patient's medical records in his or her office. But the component pieces—the patient's name, biographical information, and drug history—might be distributed and stored in different locations; without the appropriate software, the relevant information could not be assembled in a usable form.[158]

Data divisibility and data partitioning thus highlight 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 instead searching or seizing a back-up copy stored extraterritorially? Can (or more importantly, should) the United States demand that U.S.-based ISPs retain copies of their customers' data within the territorial jurisdiction of the United States so as to avoid the kinds of issues being raised by the *Microsoft* case? In a relational database, is the relevant location the place from which the data is accessed and reassembled in a usable form, or the locations where each of the component parts is stored? Under the analogous rule for tangible property, the location of each component part would control. But this would require a territoriality determination—and possibly the

---

[156] *Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations [http://perma.cc/KNK8-Y6GR]; 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) (detailing the numerous data servers operated by U.S. companies that are located outside the United States).

[157] *See, e.g.*, Ian Walden, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent* 3 (Queen Mary Univ. of London, School of Law, Research Paper No. 74, 2011), http://ssrn.com/abstract=1781067 [http://perma.cc/SA7K-J83V] ("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.pdf [http://perma.cc/488S-RZK8] (describing the benefits of partitioning). *But see* Brief for Computer and Data Science Experts, *Microsoft*, *supra* note 152, at 20-21 (noting that, while sharding and partitioning are useful for very large files, it would be highly inefficient to shard or partition email messages and then reconstitute them each time a user accesses his or her account given their small size).

[158] *See* Cauthen, *supra* note 152 (describing relational databases).

application of different rules—for the acquisition of the various fragments of a sought-after account or database. As these questions suggest, data location is both highly manipulable and, in some cases, difficult to define. The manipulability and indeterminacy of data thus undercut the normative significance and stability of data location, raising important questions as to the primacy of data location in determining the rules that apply.

C. LOCATION INDEPENDENCE

1. 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 performing the search or seizure and the location of the property being searched or seized. With the rise of modern technology, an agent conducting a search or seizure no longer need be physically located in the same place as the target of the search or seizure.[159] This section begins by analyzing how courts and the executive branch have addressed this location independence between government agents and their targets in the context of guns and drones. It then explores how data's unique features affect the analysis.

In two recent cases, U.S. border control agents located on U.S. soil shot and killed non-citizens on the Mexican side of the border. [160] In both cases, the parents of the deceased children brought, among other claims, Fourth Amendment challenges to the allegedly excessive use of force. In *Hernandez v. United States*, the Fifth Circuit (sitting *en banc*) dismissed the Fourth Amendment claim on the fact that the decedent was a non-citizen outside the United States.[161] In contrast, in *Rodriquez v. Swartz,* the Arizona district court allowed the Fourth Amendment claim to proceed given, among other things, the decedent's proximity to and familial connections with the United States.[162] Notably, even though the two courts split as to the outcome, they were in agreement as to the territoriality determination. Both courts assumed, with relatively little analysis, that, the relevant seizure took place in Mexico, where the decedent was killed, rather then the United States, where the agents who fired the shots were located. Territoriality was therefore determined by the location of the target, and both cases were presumed to involve extraterritorial action.[163]

The use of drones provides another example of the potential disconnect between government agents and their targets. Drone operators sitting in Langley,

---

[159] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491 (2014) (noting that, thanks to cloud computing, the location of the data being searched and the agent conducting the search may not be one and the same).

[160] Hernandez v. United States, 757 F. 3d 249, 255 (5th Cir. 2014) (border agent in Texas shot and killed a 15-year old Mexican); Order, Rodriguez v. Swartz, No. 4:14-CV-02251 (D. Ariz. July 9, 2015) (border agent in Arizona shot and killed 16-year old Mexican)

[161] Hernandez v. United States, 785 F.3d 117, 119 (5th Cir. 2014) (*en banc*); *see also* Hernandez v. United States, 757 F. 3d 249, 266-67 (5th Cir. 2014).

[162] Rodriguez, No 4:14-CV-02251, at 12-16.

[163] *See* Hernandez v. United States, 785 F.3d at 119; Rodriguez, No 4:14-CV-02251, at 8.

Virginia, or at any one of a number of military bases, can remotely pilot a drone and drop a bomb halfway around the world in, say, Yemen, Somalia, or Iraq. Yet virtually every legal and policy analysis of drone strikes assumes, consistent with the border shooting cases, that territoriality is determined by the location of the target. Thus, targeted killings constitute extraterritorial actions (i.e., seizures), regardless of the location of the drone operator.[164]

By straightforward analogy to guns and drones, the initial search and seizure of data would be understood to take place where the data was stored and manipulated, rather than 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 they have focused on the location of the computer where the data is stored, rather than the location of the government actor. In *United States v. Gorshkov*,[165] 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 of territoriality.[166] (Russia deemed this an extraterritorial search as well, asserting it was a violation of its domestic law and filing criminal charges against one of the FBI agents involved.[167]) As discussed in Part I.C.1, the Department of Justice, commentary on the proposed Rule 41 amendment to permit the issuance of remote search warrants, similarly accepts that the territoriality analysis depends on where the data is located—not on the location of the government agent remotely accessing or manipulating the data.[168]

But, as the government's position in the *Microsoft* case suggests, this seemingly straightforward transposal of the rules applicable to drones and guns to the world of data is contestable. There is, after all, a key difference between shooting a gun or activating a remotely controlled drone and manipulating data in the ways described in the *Gorshkov* or *Microsoft* cases. When a government agent shoots a gun across the border or launches a drone in Somalia, there is an apparent, tangible invasion of airspace and an apparent, tangible effect in another nation's territory (such as an explosion, the destruction of property, or the possible killing of individuals). 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 neither an observable effect in State *B* nor a change in the data user's ability to access and use the data.[169]

---

[164] *See, e.g.*, OLC Al-Aulaqi Memo, *supra* note 7.

[165] United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

[166] *Id.* at *3 (holding that "agents' extraterritorial access to computers in Russia and their copying of data contained thereon" was not covered by the Fourth Amendment since it was an extraterritorial action directed at a non-resident alien located outside the United States).

[167] Mike Brunker, *FBI Agent Charged with Hacking*, MSNBC, Aug. 15, 2002, http://www.nbcnews.com/id/3078784/#.VM178lph3L9 [http://perma.cc/9H5T-KZRV].

[168] *See supra* Part I.C.1; *see also* Raman Letter, *supra* note 9, at 4 ("In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), 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.").

[169] *But see, e.g.*, Walden, *supra* note 157, at 4 (noting that remote data retrieval may yield data changes, particularly when accessed through certain types of cloud-based interfaces or unknown

In fact, some have concluded that because remote access of a server does not alter or interfere with the user's ability to access his or her data, the copying of data does not amount to a constitutionally relevant seizure. Orin Kerr, for example, initially asserted that copying data is not a seizure for Fourth Amendment purposes because it leaves the data owner's possessory interests intact.[170] The magistrate judge in the *Microsoft* case agreed, and cited Kerr for the proposition that the relevant constitutional moment first occurs when the data is reviewed in the United States—not when it is merely copied.[171]

Notably, Kerr later changed his perspective, concluding that the Fourth Amendment's prohibition on unreasonable seizures is designed to regulate, among other things, the government's ability to secure and control information.[172] When copying data adds to the pool of information available to the government, it constitutes a Fourth Amendment seizure.[173] Although arguably in tensions with Supreme Court precedent,[174] several other scholars and courts have similarly concluded that the copying of electronic data constitutes a seizure.[175]

---

architecture).

[170] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 557-58 (2005). Kerr nonetheless argues that the manipulation of a computer or other device that is required to copy the data is itself a constitutionally-cognizable search. Therefore, he would still require a warrant, but on the basis of the manipulation of the machine, not the mere copying of data. *Id.* at 558, 561.

[171] *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014). The Fourth Amendment argument is a bit of a red herring, as it is largely irrelevant to the central question about warrant jurisdiction under the 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 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 the 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).

[172] *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 704 (2010) (acknowledging a change in thinking and rejecting his earlier views about whether copying constituted a seizure for purposes of the Fourth Amendment).

[173] *Id.* at 709-14.

[174] *See* United States v. Jacobsen, 466 U.S. 109, 113 (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, according to one view, unaffected. The claim, therefore, must turn on some alternative possessory interests beyond the interest in using and manipulating the data—such as the possessory interest in excluding and determining who, and under what circumstances, others are permitted to access one's property.

[175] *See, e.g.*, Brief for Amici Curiae Brennan Center for Justice at NYU School of Law, American Civil Liberties Union, The Constitution Project, and Electronic Frontier Foundation in Support of Appellant at 4, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) ("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, 113 (2002) ("Copying has an effect upon the 'ownership' rights of the party whose information is copied. For policy reasons, the copying of data should be defined as a seizure."); Paul Ohm, *The Fourth Amendment Right To Delete,* 119 HARV. L. REV. F. 10, 12 (2005) ("The right to delete explains why imaging is seizure without requiring *Hicks* to be overruled or otherwise conflicting with existing jurisprudence."); *cf.* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("It only stands to reason that, if

My point here is not to try and resolve this dispute. Rather, I use the mere fact that this is an active debate as example of the ways in which data is different. fact that this is even an active debate highlights the ways in which data is different. Unlike an explosion from a gun or a missile, the extraterritorial copying of 0s and 1s can be done surreptitiously and without any observable change to conditions in State *B*. This opens up space for the government's argument that the location of *access*, not the location of data, is what counts.

2. Disconnect Between Data and the Data User

Location independence refers to the idea that data need not be stored in the same location as, or anywhere near, its user. This allows users to access their data from wherever they are located and is central to the efficiency of the cloud. Among other benefits, location independence allows providers to move data in order to minimize the use of storage centers at peak times, avoid down servers or power outages, and perform server maintenance without disrupting user access.[176] Under current practices, providers control the location of data—generally making these location decisions without notifying the user or obtaining his or her consent each time the data is moved from one place to another. In fact, the user is often blissfully ignorant of where his or her data is stored at any given moment.

As discussed above, this raises normative questions about making data location determinative 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 linking the interests of the person to the location of his or her property falls apart. When the user has no knowledge of where his or her data is at any given moment, it is hard to claim that data location means much to the user. This disconnect 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 a 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*,[177] even when law enforcement agents locate a target's smartphone, computer, or other electronic device, they often will not know where the data stored on the device is physically being held.[178] This creates hurdles for law enforcement, for even when it has a device and all the necessary passwords, it will not necessarily be able to ascertain—thanks to the

government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search.").

[176] 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).

[177] 134 S. Ct. 2473, 2495 (2014) (holding that, absent exigent circumstances, police must obtain a warrant before searching a cell phone incident to arrest).

[178] *Id.* at 2491 ("[O]fficers 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 has been pulled from the cloud.").

cloud—whether it is accessing data that is stored territorially or extraterritorially.[179] (This problem, of course, does not arise when the government is, as in the *Microsoft* case, compelling the production of data directly from a 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 author of an email describing plans to remotely detonate explosives at an upcoming parade. The agent needs to connect the data to the device that sent the email; determine the location of the device; and then ascertain the location of the device's user, which, absent real-time tracking, may not be the same as that of the device itself. Finally, the agent may need to determine the identity of the user—that is, whether or not the user is a citizen or noncitizen 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 perform on an individualized basis.[180] 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.[181] 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 inspects 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 either no return address, a false address, and/or an address that is accurate but at which the sender is no longer located. Thus, identification problems arise even with tangible evidence. But the quantity of electronic data, the rise of anonymization tools, and the circuitous way in which data transits from place to place magnify and exacerbate the difficulties associated with user identification. These difficulties raise questions about the viability of schemes that depend on user location and identity as key to the rules that apply.

D. DATA'S INTERMINGLING

Data is also different from tangible analogs in the way it can, and often does, intermingle the property of multiple users. As discussed in Part I.B, communications transiting the fiber-optic networks are often bundled together as

[179] *See also supra* Part I.C.1 (discussing this problem in the context of remote search warrants).

[180] *See, e.g.*, Banks, *supra* note 10, at 1639 & n.47, 1645 (emphasizing the difficulty of ascertaining user location).

[181] *See supra* notes 70-75 and accompanying text.

multi-communication transactions. The NSA currently lacks the technological capacity to separate out these communications into their discrete components.[182] Thus, if any one of the multiple communications is "to," "from," or "about" a non-U.S. person that is the target of surveillance, the government will acquire 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- or 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 determination and thereby ascertaining which rules apply. Consider, for example, a Google Document that is not yet accessible to the general public but potentially accessible to multiple private users. Alternatively, consider 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 for purposes of determining the applicable rules? Should, for example, the Fourth Amendment protect the search and seizure of the Google Document if any *one* of the users is located in the United States or is a U.S. citizen or noncitizen with sufficient voluntary connections to the United States? Or should the Google Document be protected only if the *target* of the search or *all of the users* fall into this category of Fourth-Amendment-protected persons?[183]

Congress considered this issue in relation to 702 collection and placed a prohibition on the acquisition of "wholly domestic communications."—those communications in which the sender and *all* recipients are located in the United States.[184] 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. Such a rule increases the aperture of potential collection for purposes of gathering foreign intelligence information. But why should this be? Why should the 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 applicable rules further highlight the complexity of implementing the territorial and identity-based distinctions required by law.

---

[182] *See* Bates 2011 Opinion, *supra* note 75, at *10 ("[The] NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.").

[183] *See also* Kerr, *The Global Internet, supra* note 11, at 317 (warning of the possibility of "conflicting standards when more than one person has [Fourth Amendment] rights in a communication").

[184] 50 U.S.C. § 1881a(b)(4) (2012); Bates 2011 Opinion, *supra* note x, at 11;.

E. THIRD- PARTY ISSUES

Owners of tangible property tend to retain such property themselves, with only a small portion turned over to third parties to manage or execute. By contrast, we delegate large quantities of our digital property to the control of others. Vast quantities of electronic data are now held, or otherwise controlled, by third parties, including ISPs, cloud service providers, and companies that maintain and operate the fiber-optic cables that make up the Internet's backbone. Moreover, it is the third party, not the user, that generally makes the 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 the sought-after data.

According to the third party doctrine, data exposed to third parties is not protected by a reasonable expectation of privacy.[185] The doctrine originates from two 1970s Supreme Court opinions—*Smith v. Maryland*[186] and United States v. Miller.[187] But whereas the quantity and type of information at stake in *Smith* and *Miller* was limited by the relatively unsophisticated technology at the time and the facts of the cases,[188] it is no longer feasible to participate in a digital world without exposing an incredible wealth of private information—including one's associations and private thoughts—to a third party. As a result, the third party doctrine has increasingly come under attack.[189] Again, I do not seek 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 between data and 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 (and not the location of the property) potentially determinative of the rules that apply. In the *Microsoft* case, for example the government is arguing that because the Microsoft is domiciled in the United States, the government can compel the production of data under its control—irrespective

---

185 *See id.* at 443 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed.").

186 442 U.S. 735 (1979).

187 425 U.S. 435 (1976).

188 *See Smith*, 442 U.S. at 737 (collection of telephone numbers dialed on a single day); *Miller*, 425 U.S. at 437-38 (collection of four months worth of bank records).

189 *See, e.g.*, Colb, *supra* note 6, at 126-30; Richards, *supra* note 6, at 1117-19 (describing the intuitive case for protection of third-party records); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 109-15 (2008) (discussing the untenability of the Stranger Principle); Strandburg, *supra* note 10, at 619-21 (2009) (suggesting that technological change has rendered the third party doctrine untenable); *see also* 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." (citations omitted)); 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." (footnote omitted)).

of the data's location [190] rather than location of the property, potentially determinative of the rules that apply. The fact of third party control also offers a possible way to reconcile the government's position with respect to the proposed Rule 41 amendment—conceding that courts lack authority to authorize law enforcement searches of extraterritorially located data—and its position in the *Microsoft* case.[191] Even if law enforcement agents could not themselves access data located extraterritorially, the rules are different—or so the government says—if a third party performs the search or seizure.[192]

Second, third party control 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—or pass data localization laws—ensuring that data will be stored in a particular location.[193] But currently, most data users do not retain such control over their data. In fact, the efficiency of both the cloud and a global Internet depend, to a significant degree, on third parties being able to move data around in the most expeditious manner, without being constrained by user preferences and control.

III. WHAT DOES IT ALL MEAN?

As the preceding Part 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 users challenge the assumption that data location should determine the rules that apply. Why should privacy rights or law enforcement's access to sought-after evidence turn on where data happens to be located at any given moment, particularly given the near-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, identity and location-based distinctions that Fourth Amendment and surveillance law demand. Even absent the problem of multi-communication transactions, U.S. persons' and non-U.S. persons' 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* without any readily apparent violation of State *B*'s territorial integrity. From the perspective of State *B*, however, this is an arguable violation of sovereignty since State *A* is determining when, and according to what procedures and substantive standards, data located in State *B* can be seized. Such unilateral

---

[190] *See* Appellee Brief, *Microsoft*, *supra* note 1, at 9, 26-30; *see also, supra*, notes 151-152 and accompanying text.

[191] *See supra* Part I.C.1.

[192] *But see* Appellant Brief, *Microsoft*, *supra* note 145, at 30-32 (arguing that Microsoft has essentially been conscripted to do the government's bidding and therefore is operating as an agent of the government, subject to the same sets of rules).

[193] *See supra* note 155 and accompanying text.

seizing of data ignores longstanding efforts of nations—including the United States—to establish sovereign control and regulation over data within one's own territory. It also creates a possible conflict of laws and adds fuel to certain types of data localization movements.

This Part addresses the legal implications of these insights with respect to the three doctrinal fields 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 undercut the foundation of Fourth Amendment territoriality. Conversely, whereas the government argues, at least in the context of the *Microsoft* case, that longstanding territorial-based limitations on law enforcement jurisdiction should yield in the face of un-territorial data, I point to countervailing policy considerations and principles of international law that, at a minimum, complicate the government's position.

As the foregoing discussion suggests, the answers to data's un-territoriality are not, and need not be, identical across the board. But whatever one decides is the right solution, one thing is clear: data challenges the dominance of territorial-based distinctions in the law, and these challenges must 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 the *Stanford Law Review*, Orin Kerr addresses "[t]he conflict between the territorial Fourth Amendment and the facts of the global Internet."[194] But while recognizing the way in which "Internet technologies . . . disrupt[] the prior relationship between person and place,"[195] Kerr assumes that the territorial-based distinctions announced in *Verdugo-Urquidez* are correct.[196] He thus applies his Fourth Amendment theory of equilibrium adjustment—pursuant to which Fourth Amendment that adapts to technological developments by maintaining 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.[197]

---

[194] Kerr, *The Global Internet*, *supra* note 11, at 289.

[195] *Id.* at 303.

[196] *See, supra,* Part I.A; United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) ("[T]he purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside the United States territory."); *id.* at 271 ("[A]liens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country.").

[197] Kerr, *The Global Internet*, *supra* note 11, at 303-04; *see generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment,* 125 HARV. L. REV. 476 (2011) (introducing Kerr's theory of equilibrium-adjustment, which posits that the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection).

I instead suggest an alternative perspective, namely that data calls into question the primacy of location and citizenship to the application of Fourth Amendment rights.. Even if one understands the term "the people" in the way Chief Justice Rehnquist suggested in *Verdugo-Urquidez*—applying the Fourth Amendment's protections only to citizens and those with substantial connections to the United States[198]—the mobility and intermingling of data mean that territorial- and identity-based distinctions leave the "people" insufficiently protected by a territorial Fourth Amendment, at least at the stage at which data is acquired.[199] This claim is even stronger if the term "the people" is, as Justice Kennedy suggested,[200] understood to emphasize the importance of the right, rather than limit who can assert a claim. As David Gray suggests, the key question 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 in toto*—something that the search or seizure of intermingled data does, regardless of the location of the acquisition, the location of the target, or the target's identity.[201]

The following responds to Kerr's suggested equilibrium adjustments and considers two alternative responses: first, a presumptive Fourth Amendment; and second, a universalist Fourth Amendment total rejection of the territorial- and identity-based limitations, at least at the point at which data is acquired.

1. An Equilibrium-Adjusted Fourth Amendment

In applying a series of equilibrium adjustments to the Fourth Amendment, Kerr asks critical questions about how to apply a territorial Fourth Amendment in a globally interconnected world. He examines whether a person's online contacts constitute sufficient connections to the United States to trigger the application of the Fourth Amendment. [202] And he asks how the law should apply to the monitoring of communications between those with Fourth Amendment rights and those without.[203] Yet, his analysis presumes the continued desirability of a territorial Fourth Amendment. As a result, Kerr fails to fully acknowledge the degree to which data shakes the very foundation of Fourth Amendment territoriality.

Among other proposed adjustments, Kerr suggests that Fourth Amendment protections kick in so long as *either* the sender or the recipient of a communication is a U.S. person or located in the United States—those individuals

---

198 *Verdugo-Urquidez*, 494 U.S. at 265.

199 *But see* Daskal, *supra* note 32 (raising concerns about Chief Justice Rehnquist's understanding of the Fourth Amendment's reach); Kent, *supra* note 23, at 515 (noting that there is no 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 any significance from the difference in terms).

200 *Verdugo-Urquidez*, 494 U.S. at 276.

201 *See supra* notes 48-49 and accompanying text.

202 Kerr, *The Global Internet*, *supra* note 11, at 307 (arguing that online contacts do not suffice).

203 *Id.* at 313-15 (concluding that the government ought to satisfy Fourth Amendment standards when it monitors communications between those with Fourth Amendment rights and those without, but restricting this insight to communications in transit).

entitled to protection under current Fourth Amendment doctrine.[204] This is in contrast to the government's current approach, which looks exclusively to the identity and location of the *target* of the search in determining the rules governing collection.[205] 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 constitutionally reasonable under the Fourth Amendment.[206] But depending on how "good faith" is interpreted, this could become the exception that swallows the rule: Is preponderance of the evidence enough? Does good faith permit a presumption (akin to that currently employed by the NSA) that unknown parties to a communication are noncitizens lacking Fourth Amendment rights?[207]

Of additional concern, Kerr's proposed adjustment—consistent with longstanding Fourth Amendment doctrine—applies only 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.[208] At that point, the Fourth Amendment inquiry shifts exclusively to the recipient, who becomes the sole party with a continuing reasonable expectation of privacy in the communication. 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 constitutes "delivery," then Kerr's proposed adjustment will provide little-to-no protection to a key subset of "the people" whom the Fourth Amendment is meant to protect—U.S. persons sending emails to non-U.S. persons who lack Fourth Amendment rights.[209] 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.[210] But even if "delivery" is understood as 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.[211]

---

[204] *See id.* at 308-11.

[205] *See* discussion, supra, Part I.A.

[206] *Id.* at 308-10.

[207] *See also* David G. Delaney, *Widening the Aperture on Fourth Amendment Interests: A Comment on Orin Kerr's* The Fourth Amendment and the Global Internet, 68 STAN. L. REV. ONLINE 9, 10-11 (2015) (describing the complicated tailoring of good faith rules that will need to take place when dealing with the multiple government actors conducting monitoring in cyberspace).

[208] *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (citing cases); 6 WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 11.3(f) (5th ed. 2012).

[209] Kerr acknowledges this problem. *See* Kerr, *The Global Internet*, *supra* note 11, 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").

[210] *See* 50 U.S.C. § 1881a(b)(2) (2012) (prohibiting the targeting of a person reasonably believed to be located outside the United States for the purpose of gathering information about a particular, known target reasonably believed to be located within the United States).

[211] In recent litigation, the Justice Department has helpfully hinted that the destination point is receipt by the actual recipient, not just arrival at the ISP's server, which means that the sender

Thus, even with the kind of helpful adjustments suggested by Kerr, the intermingling of U.S. and non-U.S. persons' information creates a high likelihood of both error and incidental collection. Put another way, even under Chief Justice Rehnquist's conception of the Fourth Amendment, "the people" are insufficiently protected.

2. A Presumptive Fourth Amendment

A much more robust response—and the one I prefer—*presumes* that the Fourth Amendment applies regardless of whether the collection takes place inside or outside the United States, and regardless of whether 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 is a U.S. person. The presumption also applies regardless of whether the communication is in transit or not. In practice, this means that bulk collection, wherever it takes place, will fall within the Fourth Amendment's ambit; cross-border communications will 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 show that none of the parties to communication is a U.S. person. By contrast, the surveillance of North Korean diplomats in North Korea or the targeted collection on Al Nusra Front leaders in Syria is unlikely to trigger the Fourth Amendment—although there may be policy reasons to expand protection to 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. There is, I believe, a legitimate foreign intelligence exception to the warrant requirement in some circumstances.. Rather, my argument is that Fourth Amendment protections, however defined, ought to apply to U.S.-person targets and non-U.S.-person targets alike, absent clear and convincing evidence that collection does not encompass communications to or from a U.S. person or include other data (such as stored documents) that have been generated in whole or in part by a U.S. person.

To be more concrete: if a warrant based on probable cause is required to collect the content of electronic communications, it should presumptively be required across the board, to both citizen and noncitizen targets—irrespective of the location of the data or the target. Absent a determination that the communication *exclusively* takes place between non-U.S. persons, the warrant requirement should apply. Conversely, if a warrant is not required to collect certain types of information (such as certain types of foreign intelligence information or dialed phone numbers) this exception should also apply across the board—to citizens and noncitizens alike—regardless of where the data or the target is located.

---

retains a reasonable expectation of privacy until the communication is actually received by the recipient. *See* Government's Unclassified Response to Defendant's Alternative Motion for Suppression of Evidence & a New Trial at 48 n.32, United States v. Mohamud, No. 3:10-CR-00475-KI-1 (D. Or. June 24, 2014), 2014 WL 4792313, at *24.

Such a proposal will undoubtedly engender objections. It would be, after all, a dramatic change in the way the government thinks about its obligations toward non-U.S. persons outside the United States. However, the United States is already moving in that direction, albeit as a matter of policy, not law. A recently issued Presidential Policy Directive (PPD-28) directs the intelligence community to establish post-acquisition limits on the dissemination and retention of collected data.[212] It requires that these safeguards apply "equally to the personal information of all persons, regardless of nationality," to "the maximum extent feasible consistent with the national security."[213] The policy directive applies across the board, even in those situations where all parties to a communication are non-U.S. persons. A presumptive Fourth Amendment would thus extend the already existing policy of post-acquisition restrictions on use, dissemination, and retention to the level of collection itself. And it would do so as a matter of law.

Some will object that applying the Fourth Amendment's protections to the collection of noncitizens' data overseas will impede the government's ability to gather critical foreign intelligence information essential to the nation's security. 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 "touchstone" of Fourth Amendment analysis[214]—is a flexible standard that takes into account the governmental interest at stake. Even in the context of domestic law enforcement, where Fourth Amendment interests are at their zenith, the doctrine generally provides law enforcement agents significant latitude to search and seize.[215] A presumptive Fourth Amendment still permits the government to search and seize the data of non-citizens for a wide array of law enforcement and intelligence purposes; it simply prohibit *unreasonable* searches or seizures of data any time a U.S persons communications are potentially implicated. This is a necessary means of indirectly protecting "the people" who fall within the Fourth Amendment's ambit.

Others will suggest that minimization rules restricting the use, retention, and dissemination of acquired U.S. persons' information sufficiently address the Fourth Amendment concerns I have identified. But while minimization rules are undoubtedly important, they protect separate interests. Whereas acquisition rules

---

[212] *See* PPD-28, *supra* note 19.

[213] *See id.* § 4(a), *supra* note 19; *see also* David Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y, 209, 289 (2014) (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 [http://perma.cc/C599-Q7ZX] (suggesting that the policies required are already largely consistent with current practice).

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

[215] *See, e.g.*, Kerr, *New Technologies*, *supra* note 10, at 828 (noting the "relatively modest and deferential Fourth Amendment in the area of developing technologies"); *Warrantless Searches and Seizures*, *supra* note 39 (describing the many exceptions to the warrant requirement); *supra* note 189 (addressing the breadth of the third party doctrine).

define the government's ability to gather information, minimization rules govern what the government can do with the information upon its acquisition. Acquisition has the capacity to both alter the balance of power between the governed and the government and to chill speech and association, among other consequentialist harms. The acquisition of data should thus be understood as independently implicating the Fourth Amendment rights of U.S. persons, regardless of the existence—or not—of other separate restrictions on use, retention, or dissemination. In fact, Congress has implicitly recognized the ways in which acquisition itself implicates the rights and interests of "the people" in its detailed rules governing the acquisition of electronic and stored communications.[216]

To reiterate, this position does not assume all electronic surveillance or seizure of data triggers the Fourth Amendment. Nor does it assume that a warrant is required any time the Fourth Amendment is triggered. There is, after all, an important and ongoing debate about when the Fourth Amendment protects electronic communications and other types of data.[217] The claim is simply that whatever answers we arrive at should presumptively apply to U.S. persons and non-U.S. persons alike, regardless of whether the target of the acquisition or the data being acquired is based in the United State—absent a determination that all parties to the communication are non-U.S. persons. In many cases, noncitizens will be entitled to the protections of the Fourth Amendment, not because they are subsumed within "the people," but in order to protect citizens and other persons with sufficient connections to the United States that current constitutional doctrine teaches are entitled to the Amendment's protections.

3. A Universalist Approach

Another possible response—what I am labeling the universalist approach—is a total rejection of the Fourth Amendment's territorial and identity-based limitations. Proponents of this universalist approach have two dominant rationales. The first is to provide an a bright line prophylactic response to the risk of incidental collection without the possibility of exceptions. The second is the larger aim of repudiating of Chief Justice Rehnquist's conception of "the people" as limited to those with sufficient voluntary connections to the United States.[218]

There are two possible versions of the universalist approach. Under the stronger version, what I call "pure universalism," all targets of U.S. actions are treated equally. Under the second, the Fourth Amendment applies regardless of the location or identity of the target, but location or identity still play a role in

---

[216] *See supra* Part I.B-C.

[217] *See supra* note 189 and accompanying text (discussing ongoing debate on the third party doctrine); *see also* United States v. U.S. 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 [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (holding that "a foreign intelligence exception to the Fourth Amendment's warrant requirement exists" in specified circumstances).

[218] *See, e.g.*, Alec D. Walen, *Fourth Amendment Rights for Nonresident Aliens*, GER. L.J. (forthcoming) (manuscript at 21-25), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2533582 [http://perma.cc/B25Z-SW9E] (arguing that Chief Justice Rehnquist misinterpreted the meaning of "the people").

determining *how* the Fourth Amendment applies (e.g., when a warrant is required).[219] As is obvious, only the first version (pure universalism) fully responds to the unique features of data identified in this Article. The second approach applies the Fourth Amendment to noncitizens located outside the United States, but then re-introduces territorial and identity-based inquiries into a later stage of analysis. But problems of target identification and intermingling apply regardless of the stage at which the inquiry takes place.

This universalist approach differs from the presumptive approach in that it would apply the Fourth Amendment even to the collection of "wholly" non-citizen, non-resident communications. It would thus apply even when the government could show that the acquisition covers North Koreans talking to North Koreans, and no U.S. person communications will be incidentally acquired.

While this approach has the arguable benefit of simplicity, it also runs headlong into current doctrinal understandings that limit the application of the Fourth Amendment to those with substantial voluntary connections to the United States. Regardless of what one thinks of Chief Justice Rehnquist's fairly cursory explanation of the textual, historical, and normative justifications for his limited conception of "the people," his reasoning has since become entrenched in the doctrine, with lower courts and legislators repeatedly relying upon his analysis.[220] The judiciary, executive branch, and Congress are not likely to readily embrace the idea that the Fourth Amendment applies to communications that are *known* to involve exclusively noncitizens located outside the United States.

By comparison, a presumptive Fourth Amendment achieves much of what a universalist Fourth Amendment strives toward, but does so without requiring a total overhaul of current doctrine. After all, a world of highly mobile and intermingled data, *Verdugo-Urquidez* is failing on its own terms; a set of strong presumptions is needed to protect "the people" that are, according to the Court's reasoning in *Vergudo-Urquidez,* entitled to the Fourth Amendment's protections. Under this approach, the Fourth Amendment thus presumptively applies; the burden is on the government to establish that acquisition is limited to the extraterritorial acquisition of non-U.S. person data only. Unless the government is engaged in the targeted collection of extraterritorially-located non-citizens communicating exclusively with extraterritorially-located non-citizens (such as the targeted collection of North Koreans talking to other North Koreans), the Fourth Amendment will presumptively apply.

B. FOREIGN SURVEILLANCE: ADDITIONAL CONSIDERATIONS

Recommendations with respect to the statutory requirements governing foreign intelligence surveillance track 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

[219] *See, e.g.*, Delaney, *supra* note 207, at 14-15 (suggesting support for a universally applicable Fourth Amendment in cyberspace but also suggesting that the standards as to what satisfies the Fourth Amendment may differ for U.S. citizens and non-citizens, thereby making identify determinative of *how* the Fourth Amendment applies).

[220] *See supra* notes 31-32 and accompanying text.

protections for all, at least at the acquisition stage.[221] This insight has only grown more salient over time, as the Internet has become a truly global network. Congress should thus rewrite FISA to set universally applicable requirements for acquisition that no longer depend on the location of the data or identity of the target.

Again, my purpose here is not to lay out the specific rules that ought to be adopted—that is beyond the scope of this Article. Perhaps warrants should be required; perhaps not. Or perhaps there is a middle ground, in which warrants are required for certain types of acquisition. But whatever the rules, they ought to be applied universally, absent clear and convincing evidence that none of the parties to the communication is a U.S. citizen or legal permanent resident.

At the same time, Congress should turn its attention to the critically important—and largely neglected—question of use.[222] 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 focuses almost entirely on the rules governing collection, giving scant attention to rules governing the access and use of collected data. For example, while Congress mandates the development of so-called minimization rules to govern the access to, retention, and dissemination of U.S. persons' information, it delegates the development of these specific procedures to the Attorney General, subject to approval by the FISC.[223] The overarching requirements are written at such a level of generality that they effectively delegate all the key details to the executive branch.[224] This is a mistake. So long as foreign intelligence collection continues to be as sweeping as it has been of late, minimization rules and use restrictions are critical. Thus, while this Article (like Congress) is focused primarily on acquisition and not use, the two must go hand-in-hand.

Meanwhile, Congress ought to embrace the reality of data's intermingling and rewrite its acquisition rules to turn on factors (such as type of information being collected) that do not depend on the identity or location of the target. As it does so, it should consider the definition of foreign intelligence. The broader the definition, the harder it will be to justify a warrant exception for foreign intelligence surveillance, particularly given its application to U.S. persons and non-U.S. persons alike. Conversely, the narrower and more limited the definition of foreign intelligence, the easier it will be to justify warrantless surveillance for foreign intelligence purposes.

---

221 *See supra* notes 57-58 and accompanying text.

222 *See, e.g.*, Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, Foreign Aff. (March/April 2014); Banks, *supra* note 10, at 1660, 1637 (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). These use questions tend to fall under the rubric of post-acquisition minimization rules, discussed *supra* in Part I.B.

223 *See* 50 U.S.C. § 1881a(e) (2015).

224 *See* 50 U.S.C. § 1801(h) (2012) (defining the required "minimization procedures").

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 longstanding principle that nations are prohibited from unilaterally exercising their law enforcement jurisdiction in another nation's territory, as well as an awareness of the diplomatic consequences and practical difficulties of doing so.

Notably, both sides in the *Microsoft* case argue that they respect the territorial-based limits of the government's warrant authority. They just differ as to the question of whether certain actions occur territorially or extraterritorially, at least for purposes of the Stored Communications Act. Microsoft argues by analogy to the territorial-based limits applicable to warrants issued under Federal Rule of Criminal Procedure 41 and rules governing the search and seizure of tangible property.[225] 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.[226] 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 a "hybrid warrant"—part warrant and part subpoena. Analogizing to the rules governing subpoenas, the government argues that it is the location of the entity (Microsoft) with control over the data that matters.[227] Both sides cite policy reasons as to why their interpretation is the correct one.[228]

The *Microsoft* case thus pits the location of data 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. Yet neither approach is fully

---

[225] *See* Appellant Brief, *Microsoft*, *supra* note 145, at 36-37, 41-45.

[226] 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* Appellant Brief, *Microsoft*, *supra* note 145, at 38 ("Congress must be presumed to have been aware of these plain—and plainly different—meanings when it used these terms in sequential provisions of ECPA. The district court erred in indulging exactly the opposite presumption—that Congress imported into the word 'warrant' principles that courts had applied only to the very different device called a 'subpoena.'").

[227] *See* Appellee Brief, Microsoft, *supra* note 1, at 9; *see also In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft*,* 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014) ("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.").

[228] *See* Appellant Brief, *Microsoft*, *supra* note 145, at 41-57; Appellee Brief, *Microsoft*, *supra* note 1*,* at 48-57.

satisfactory.[229] Microsoft's position—pursuant to which law enforcement access to evidence depends on the location of data—yields bizarre results. Under Microsoft's approach, law enforcement access to evidence depends on an 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 for law enforcement agents investigating crimes. Moreover, the Microsoft position, while at times framed as an alternative to data localization, would likely fuel a certain kind of data localization; foreign governments would increasingly demand that ISPs store their nationals' data within their jurisdiction so as to avoid the reach of foreign law enforcement.[230]

But the government's answer—that the location of access controls—carries its own set of significant costs. 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 upon the state in which the data is stored (Ireland), without considering the applicable privacy protections and rules governing law enforcement's access to data in the state where the data is stored. This has several negative policy implications.

First, it conflicts with the international law prohibition against the unilateral exercise of extraterritorial law enforcement jurisdiction and ignores the longstanding sovereign interest in setting privacy protections for those within the nation's territory.[231] 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.[232] The United States'

---

[229] 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 145, at 34-35.

[230] *See e.g.*, Chander & Lê, *Data Nationalism*, *supra* note 155 (describing dangers of data localization); 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), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275 [http://perma.cc/D2FC-F29Y] (describing the rise of data localization movements and analyzing the key motivating factors)

[231] *See supra* Part I.C.

[232] *See* Appellant Brief, *Microsoft*, *supra* note 145, at 17-18; Brief of Amicus Curiae AT&T Corp., Rackspace US, Inc., Computer & Communications Industry Assoc., i2Coalition, and Application Developers Alliance in Support of Appellant Microsoft Corp. at 2, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) (warning that "[i]f foreign governments were to respond in kind, they could, for example, order a foreign Microsoft subsidiary to obtain and disclose to foreign authorities any private customer information . . . , applying only foreign legal standards to the question," and thereby undercutting U.S.-based statutory protections designed to "ensure the continued vitality of the Fourth Amendment"); Brief of BSA, The Software Alliance, The Center for Democracy and

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 (let's say 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?[233] Or consider the likelihood of U.K. law enforcement, pursuant to newly enacted authority, seeking to compel ISPs to directly turn over data stored in the United States, without regard to the SCA's requirement of warrant and probable cause.[234]

Third, such a scenario—with both the requesting state and the state where data is stored claiming jurisdiction over the data—creates an almost inevitable conflict of laws. ISPs can find themselves caught between two conflicting legal obligations, perhaps even with criminal consequences.[235] While this is not new—and there is an entire body of law designed to deal with such conflicts[236]—it puts ISPs in an increasingly difficult position. Fourth, the U.S. position risks its own form of data location—pursuant to which nations require that their nationals store data with locally based ISPs so as to ensure that the data is subject to that nation's

---

Technology, Chamber of Commerce of the U.S., The National Assoc. of Manufacturers as Amicus Curiae Supporting Appellant Microsoft Corp. at 16, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 15, 2014) [hereinafter BSA Amicus Brief, *Microsoft*] (warning that "the government's approach—if upheld by this Court—is likely to produce a substantial reduction in Americans' privacy as well" since "[o]ther countries will assert the same authority that the government does . . . contending that their domestic legal processes may compel production of Americans' data stored in this country").

233 *Cf.* Marketa Trimble, *The Future of Cybertravel: Legal Implications of the Evasion of Geolocation*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.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.").

234 *See* Data Retention and Investigatory Powers Act 2014 § 4(4) (Eng.). The legislation specifies that "regard is to be had" to a possible conflict of laws, although the legislation does not 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. 795, at 151 (UK) (describing a key goal of the legislation as permitting access to otherwise difficult-to-obtain data held by U.S.-based providers).

235 *See, e.g.*, Amazon Amici, *Microsoft*, *supra* note 145, at 17-18 (warning that "allowing the decision below to stand would leave cloud services providers to confront the Hobson's choice of either (a) disobeying the ECPA warrant in order to comply with the privacy laws of the country where the relevant documents are located or (b) violating those laws in order to comply with the warrant").

236 *See, e.g.*, RESTATEMENT (SECOND) OF CONFLICT OF LAWS (1971); RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW (1965); Lea Brilmayer, *The Extraterritorial Application of American Law: A Methodological and Constitutional Appraisal*, 50 LAW & CONTEMP. PROBS. 11, 12-14 (1988) (explaining the relationship between, and the scope of, the respective Restatements); Harold G. Maier, *Extraterritorial Jurisdiction at a Crossroads: An Intersection Between Public and Private International Law*, 76 AM. J. INT'L L. 280, 318 (1982) (arguing that international conflict of law problems should be evaluated "in the light of effective principles of transnational organization, not solely in terms of whether a given decision may create short-term disharmony between the nations involved"). *See also* Berman, *The Globalization of Jurisdiction*, *supra* note 10, at 329-423 (2002) (describing the range of choice of law and conflict of law issues arising in the context of an increasingly interconnected world, as well as proposed responses).

jurisdiction. (This is in contrast to the localization movements that demand the local storage of *data*; this type of movement focuses on the *ISP* location.) The economic fallout for U.S. businesses could be significant,[237] and the Internet's efficiency would suffer as well.[238] Finally, and ironically, if such movements are ultimately successful in creating closed-off or locally-controlled networks, law enforcement access to sought-after data will be compromised. The very thing that the government is seeking to do in the *Microsoft* case—compel a U.S.-based ISP to turn over data located extraterritorially—will be nearly impossible because that data will be held in closed-off networks. Put differently, the government's insistence on unilateral access to the data may undermine its ability to ever compel such data.

Taken together, these concerns highlight the need for new cross-border mechanisms that facilitate law enforcement access to data, yet also respect the sovereign interest in setting privacy protections and controlling law enforcement operations within one's jurisdiction.[239] There are several ways to achieve this balance. Here, I address some of the key considerations.

The first and most discussed—and also largely non-responsive—proposal is simply to expand the Mutual Legal Assistance Treaties (MLAT) system, pursuant to which law enforcement officials can make formal requests for cross-border law enforcement assistance.[240] It is, after all, Microsoft's position that the U.S.

---

[237] *See* BSA Amicus Brief, *Microsoft*, *supra* note 232, at 18-19 (warning of the costs to the cloud computing industry and U.S. business in particular if businesses and individuals believe that use of U.S.-based providers means a loss of privacy and confidentiality); Chander & Lê, *supra* note 155 (detailing negative impacts of localization movements). These are not hypothetical concerns. 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* 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 [http://perma.cc/W4BN-J89Q]; Anton Troianovski & Danny Yadron, *German Government Ends Verizon Contract*, WALL ST. J., June 26, 2014, http://www.wsj.com/articles/german-government-ends-verizon-contract-1403802226 [http://perma.cc/SU48-CWFT]. In fact, recent reports suggest that related concerns about U.S. surveillance practices for foreign intelligence purposes could cost the American cloud computing industry $22 to $35 billion over the next three years as foreign customers abandon or choose other providers. *See* Daniel Castro, THE INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? (2013), http://www2.itif.org/2013-cloud-computing-costs.pdf [http://perma.cc/5QXK-DJJP]; Danielle Kehl et al., NEW AMERICA'S OPEN TECH. INST., SURVEILLANCE COSTS: THE NSA'S IMPACT ON THE ECONOMY, INTERNET FREEDOM & CYBERSECURITY (2014), https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf [https://perma.cc/3HCT-GZPM]. While these reactions are at primarily motivated by the scope of the United States' foreign intelligence surveillance, a rule allowing U.S. law enforcement to unilaterally reach into other nations' jurisdictions may exacerbate the reaction.

[238] *See* Chander & Lê, *supra* note 155, at 679-82; Hill, *supra* note 230, at 4.

[239] *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 [http://perma.cc/W8J3-YYVG].

[240] *See, e.g.,* ANDREW K. WOODS, GLOB. NETWORK INITIATIVE, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE (2015), https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf; Swire &

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 violate international law.[241] This is also Ireland's position.[242] 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, for example, takes an average of ten months to respond to law enforcement requests made pursuant to the MLAT process; other nations take longer.[243] Moreover, MLAT coverage is not universal; for example, the United States has MLATs with only about half the countries in the world.[244] These processes can, and clearly should, be improved. The European Convention on Cybercrime (commonly known as the "Budapest Convention"), for example, provides a mechanism for nations to expedite and facilitate preservation orders and cross-border sharing of information;[245] these can be expanded to cover other criminal matters as well. Increased resources, including money and personnel, are also needed. Legislation currently pending in Congress mandates the creation of an online tracking system; [246] other nations should consider adopting online tracking systems as well.

However, MLAT reform, in and of itself, is not a remedy to the issues raised by the *Microsoft* case. After all, the MLAT system provides a mechanism for one government to formally request data subject to another sovereign's jurisdiction. It thus kicks in where jurisdiction ends. One still needs to answer the key underlying question: when and in what circumstances a sovereign can claim lawful jurisdiction over data, even if that data is physically located outside its

---

Hemmings. *See, e.g.*, Peter Swire & Justin D. Hemmings, Re-Engineering the Mutual Legal Assistance Treaty Process (May 14, 2015) (unpublished draft) (on file with author); [https://perma.cc/MUJ5-2MUZ].

241 Appellant Brief, Microsoft, *supra* note 145, at 17, 57-60.

242 *See* Brief for Ireland as Amicus Curiae Supporting Appellant at 4, 7, *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. Dec. 23, 2014).

243 *See, e.g.*, RICHARD A. CLARKE ET AL., PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'N TECH., LIBERTY AND SECURITY IN A CHANGING WORLD 226-29 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/36EE-6J9F] (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); Jonah Force Hill, Feature, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SECURITY J. (2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ [http://perma.cc/F5M5-APAS] ("[I]t takes an average of ten months for DOJ to process MLAT requests, and can take years. Foreign countries' MLAT requests are similarly drawn out, and can take far longer.").

244 *See* BUREAU FOR INT'L NARCOTICS & LAW ENF'T AFFAIRS, U.S. DEP'T OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT VOLUME I: DRUG AND CHEMICAL CONTROL (2012), http://www.state.gov/documents/organization/187109.pdf [http://perma.cc/FN5G-D2C2] (listing countries with whom the U.S. has entered Mutual Legal Assistance Treaties).

245 Council of Europe Convention on Cybercrime, *opened for signature* Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2006), E.T.S. No. 185, arts. 17-18, 32 (entered into force July 1, 2004)

246 The Law Enforcement Access to Data Stored Abroad (LEADS) Act, S. 512, 114th Cong. § 3 (2015).

territory. If (as is often assumed and as argued by Microsoft[247]) the location of data controls for purposes of the MLAT, then MLAT reform is only a partial solution at best. Such a response fails to account for the mobility, manipulability, and divisibility of data addressed in detail in Part II of this article.

Alternative jurisdictional triggers need to be considered, such as the place where the company controlling the data operates or maintains its headquarters, user nationality, or user location. Jurisdiction could also be based on the nature of the crime and the requesting government's interest in prosecution, rather than, or in addition to, other possible factors. My goal here is not to rank or comprehensively evaluate the various options—each of which carries its own challenges—but simply to identify some of the possible choices.

As *process* matter, it seems these jurisdictional questions are best dealt with through a series of bilateral or multilateral agreements among a handful of like-minded nations. While some are calling for an international treaty as a way to resolve such questions, [248] it will be hard—if not impossible—to achieve broad international consensus on these issues in the short-term. Any agreement that did emerge would almost certainly result in a watering down of protections, at least as compared to the warrant standard for content data stored in the United States. [249] Bilateral and small multi-lateral agreements would allow the United States and other key partners to begin to set the applicable jurisdictional, procedural, and substantive requirements, without having to try to achieve total consensus as to the outcome. If successful, these agreements would set a precedent that would be mimicked by others, eventually coalescing into broadly applicable international norms and standards.

As to the *substance* of the agreements, a few key considerations are in order: First, it seems that one of the key problems stems from a disconnect between the jurisdictional tests for data *protection* and data *compulsion*. The United States, for example, acknowledges territorial-based limitations on its regulatory authority under the Stored Communications Act,[250] yet asserts (in the *Microsoft* case) that it can compel production of data wherever located, so long as it has jurisdiction over the provider. It is precisely this double standard that is causing the potential

---

[247] *See* Appellant Brief, *Microsoft*, *supra* note 145, at 57-58.

[248] *See, e.g.,* Smith, supra, not 255; Kate Westmoreland, *A New International Convention on International Legal Cooperation* , ACS Blog, Sep. 2, 2015 (calling for a new international convention, but also acknowledging the difficulties in doing so and suggesting a range of shorter-term measures as well)

[249] An alternative—but highly implausible—response is to try to bypass these difficult jurisdictional questions, at least in certain types of cases, through the creation a new global warrant system for data. But apart from the almost insurmountable logistical difficulties (i.e., who would issue the warrant? How would national law enforcement agencies trigger the application of such a warrant), it is near impossible to conceive of a set of internationally agreed-upon procedural and substantive standards. Any such agreement would almost certainly involve a watering down of U.S. standard of warrant based on probable cause, meaning other nations could presumably gain access to data that U.S. agents could only obtain upon meeting the heightened Fourth Amendment requirements. Moreover, even if such a system were put in place, it would presumably only apply to certain types of requests or cases, still leaving the key jurisdictional questions unresolved.

[250] *See*, *supra*, Part I.C.iii.

conflicts of law and sovereignty concerns raised by the *Microsoft* case.[251] Nations should seek to of a uniform jurisdictional test that applies to both regulation and compulsion alike.[252]

Second, a key set of questions arises as to the substantive and procedural mechanisms by which one nation can demand production of data located in another nation's jurisdiction (however that is ultimately defined). Under U.S. law, for example, foreign governments must meet U.S. requirements of a warrant based on probable cause to access the content of communications stored within the United States' borders.[253] This raises a host of critical questions: When, if ever, should requesting states be permitted to obtain data held within the United States' jurisdiction based on something less than probable cause or absent sign-off by a U.S. magistrate? What minimal substantive requirements should be required? What minimal procedural requirements? Should those requirements turn on either the nature of the data or the purpose for which it is being collected? One possible response is the "bilateral parity" solution proposed by Stephen Schulhofer. Under this arrangement, each state would be required to provide other state's citizens the same protections it provides its own.[254] This solution addresses the difficulties of harmonizing multiple, diverse systems, yet also ensures that participating states agree to subject themselves to whatever substantive and procedural standards are applied.

Third, any such agreements need to address *recipient* process questions (a distinct issue than the procedural standards applicable to the requesting government). To whom should the requests be made? Under U.S. law, foreign governments seeking the content of the communications must work through the U.S. government. But they can obtain non-content data directly from the companies themselves. Should foreign governments ever be permitted to access data directly from U.S-based providers? Should limits be placed on when foreign governments can directly request non-content information?[255] There are obvious efficiency gains in permitting direct company compulsion. But there are also costs in terms of accountability and oversight.

Finally, an institutional point: whatever one decides is the best approach, the policy and diplomatic reverberations will be global. These are decisions that should be made by the political branch, not unelected federal judges. Put bluntly, however the Second Circuit comes out in *Microsoft*, Congress and the executive

---

[251] *See* David Kris, *Preliminary Thoughts on Cross-Border Data Requests,* Lawfare, Sep. 28 2015 (raising concerns about the divergence between the jurisdictional scope of what he calls "surveillance prohibitions" and "surveillance compulsions").

[252] That said, there may also be good reason for a divergent approach to regulation and compulsion. I do not seek here to tackle all of the complex factors raised by these jurisdictional tests—something I hope to do in later work—but rather seek only to identify the issues.

[253] 18 U.S.C. 2702; 2703(a).

[254] *See, e.g.,* Schulhofer, *supra* note **Error! Bookmark not defined.**, at 26 ("Instead of working toward a comprehensive multilateral framework . . . any nation could negotiate a bilateral agreement with any other, with each party merely committing to extend to citizens of the other whatever safeguards it observed in connection with surveillance of its own citizens.").

[255] *See, e.g.,* Greg Nojeim, *MLAT Reform: A Straw Man Proposal* , ACS Blog, Sep. 3, 2015 (suggestion that more sensitive non-content data, such as transactional records, should be treated like content and therefore subject to a government-to-government disclosure scheme)

need to engage.[256] A win for Microsoft would impose a set of territorial-based rules onto un-territorial data. This outcome fails to reflect the unique features of data and would likely fuel data localization movements, which in turn undercut the overall efficiency of the Internet. Conversely, a win for the government would establish a dangerous precedent under which nations can unilaterally—without agreed-upon substantive or procedural standards—compel the production of data located anywhere in the world simply by asserting jurisdiction over the company controlling the data.

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 which "here" and "there" matter. This Article exposes the ways in which data undercuts longstanding assumptions about the territorial reach of the Fourth Amendment, the viability of territorial-based distinctions in surveillance law, and the territorial limits to judges' warrant authority. But just as the challenges posed by data are multi-layered and complex, so too 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, the executive should not run roughshod over territorial-based limitations with respect to law enforcement jurisdiction, but should instead engage key foreign partners and seek consensus for a new approach.

[256] Notably, I am not alone in this sentiment. See, e.g., Oral Argument, 2d Cir. Tr. At 95 (Judge Lynch urging Congress to engage).