ARTICLES

THE FOURTH AMENDMENT AND THE GLOBAL INTERNET

Orin S. Kerr*

This Article considers how Fourth Amendment law should adapt to the global nature of Internet surveillance. It focuses on two types of problems not yet addressed by courts. First, the Supreme Court's decision in United States v. Verdugo-Urquidez *prompts several puzzles about how the Fourth Amendment treats monitoring on a worldwide network where many lack Fourth Amendment rights. For example, can online contacts help create those rights? What if the government mistakenly believes that a target lacks Fourth Amendment rights? How does the law apply to monitoring of communications between those who have and those who lack Fourth Amendment rights? The second category of problems follows from different standards of reasonableness that apply outside the United States and at the international border. Does the border search exception apply to purely electronic transmission? And if reasonableness varies by location, is the relevant location the search, the seizure, or the physical person?*

This Article explores and answers these questions using equilibrium-adjustment, a method of applying the Fourth Amendment to technological changes to maintain the preexisting balance of constitutional protection. Fourth Amendment doctrine is heavily territorial: connections to the United States impact the scope or existence of constitutional protection. This Article aims to adapt existing principles for the transition from a domestic, physical environment to a global, networked world. It concludes that courts should reject online contacts as a basis for Fourth Amendment protection; allow monitoring when the government wrongly but reasonably believes that a target lacks Fourth Amendment rights; and limit monitoring between those who have and those who lack Fourth Amendment rights. It also contends that the border search exception should not apply to electronic transmission and that reasonableness should follow the location of data seizure. Taken together, the solutions offered in this Article provide a

* Fred C. Stevenson Research Professor, George Washington University Law School. Thanks to Jack Goldsmith, Matthew Stephenson, Matthew Waxman, David Pozen, Samuel Rascoff, Robert Chesney, Jon Michaels, Josh Chafetz, Rebecca Ingber, Daphna Renan, Felix Wu, Brett Frischmann, Jennifer Granick, Christopher Soghoian, Margaret Chon, Jane Bambauer, and participants at the Privacy Law Scholars Conference for comments on an earlier draft. Thanks to Derek Woodman for research assistance.

set of Fourth Amendment rules tailored to the reality of global computer networks.

INTRODUCTION

In the last decade, courts and scholars have begun to address how the Fourth Amendment applies to the Internet.[1] They have raised and tentatively answered questions such as whether Internet users have Fourth Amendment

1. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 283-88 (6th Cir. 2010) (concluding that e-mails are protected under the Fourth Amendment); United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (concluding that files made available over a file-sharing network are not protected); United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008) (concluding that Internet Protocol (IP) addresses and to/from e-mail information are not protected under the Fourth Amendment); United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (concluding that the contents of a computer connected to a university network are normally protected); United States v. Post, 997 F. Supp. 2d 602, 606 (S.D. Tex. 2014) (concluding that the metadata embedded in a photograph posted to a website is not protected). For scholarly perspectives, see, for example, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121; Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); and Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591 (1997).

protection in e-mail,[2] whether the Fourth Amendment limits the monitoring of visited websites,[3] and whether users have Fourth Amendment rights in their subscriber data stored with service providers.[4] The law is still evolving, and the Supreme Court has yet to weigh in. But the basic parameters of how the Fourth Amendment applies to the Internet have been at least tentatively answered.

Now consider an important wrinkle. So far, almost all of the cases and scholarship applying the Fourth Amendment to the Internet have assumed domestic territoriality.[5] They assume that all of the people, data, and computers are physically located inside the United States. In the early Internet era, that assumption was natural. In the 1980s and 1990s, access to the Internet was dominated by U.S. services such as CompuServe and America Online.[6] For the most part, "the Internet" was a U.S.-based Internet, dominated by U.S.-based companies and U.S.-based users.

That assumption is now obsolete. The last twenty years have witnessed a dramatic globalization of the Internet. At the end of 2013, less than 10% of the world's Internet traffic was attributable to U.S.-based users.[7] Even U.S.-based Internet services now serve predominantly foreign customer bases. For example, 83% of Facebook's users are located outside the United States.[8] Facebook is the most popular website in dozens of countries, including Argentina, Egypt, and Pakistan.[9] Similarly, approximately 70% of Gmail's users are outside the United States, including about 9% in India and around 3% each in Japan, Rus-

---

2. *See, e.g.*, *Warshak*, 631 F.3d at 283-88.

3. *See Forrester*, 512 F.3d at 509-11.

4. *See* United States v. Christie, 624 F.3d 558, 573-74 (3d Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008); Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001); United States v. Hambrick, 225 F.3d 656, No. 99-4793, 2000 WL 1062039, at *2-4 (4th Cir. Aug. 3, 2000) (unpublished table decision).

5. There are rare exceptions, such as a 2001 case involving U.S. agents that accessed files stored on a Russian server. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (holding that the Fourth Amendment did not apply to the search of the Russian server). The very limited scholarship that has touched on these issues includes Scott J. Glick, *Virtual Checkpoints and Cyber*-Terry *Stops: Digital Scans to Protect the Nation's Critical Infrastructure and Key Resources*, 6 J. NAT'L SECURITY L. & POL'Y 97 (2012), and Stewart M. Young, Comment, Verdugo *in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases*, 10 MICH. TELECOMM. & TECH. L. REV. 139, 150-52 (2003).

6. *See* Anne Marriott, *Three-Way Deal to Put Top Rival in AOL Hands*, WASH. TIMES, Sept. 9, 1997, at B8.

7. *See Internet Usage Statistics, Population and Telecom Reports for the Americas*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats2.htm (last visited Jan. 28, 2015) (estimating that, as of December 2013, only 268,507,150 of the world's 2,802,478,934 Internet users came from the United States).

8. *See id.* (reporting that 163,817,940 of Facebook's 975,943,960 users worldwide are in the United States).

9. Michael B. Kelley, *The World's Most Popular Web Sites by Country [MAP]*, BUS. INSIDER (Oct. 4, 2013, 8:46 AM), http://www.businessinsider.com/the-worlds-most-popular-web-sites-2013-10.

sia, and Brazil.[10] Many large U.S. providers have servers all around the world to account for their largely foreign customer bases.[11]

The shift to a global Internet has major implications for the future of Fourth Amendment law. Existing cases applying the Fourth Amendment outside the United States indicate that connections to U.S. territory play a significant role in defining protections. Judicial decisions have limited who receives Fourth Amendment protection by requiring a voluntary connection to the United States as a sovereign.[12] Precedents have limited where the Fourth Amendment applies by giving U.S. authorities broad powers to investigate at the international border.[13] Still other precedents have limited how the Fourth Amendment applies overseas, replacing the usual warrant requirement with a reasonableness balancing test when U.S. authorities conduct monitoring outside the United States.[14]

The global Internet brings new salience to the extraterritorial scope of the Fourth Amendment. Territorial concerns that arose only rarely have become increasingly important. Recent disclosures by former National Security Agency (NSA) contractor Edward Snowden hint at the dynamic.[15] As the Snowden disclosures emphasize, the NSA conducts monitoring of Internet activity around the world.[16] And issues for today's NSA will likely become matters for tomorrow's law enforcement. For example, in January 2014, a criminal defendant named Jamshid Muhtorov moved to suppress Internet surveillance of his communications collected outside the United States.[17] Muhtorov, a permanent resident alien from Uzbekistan, was communicating from inside the United States with terrorist suspects abroad when his communications were intercepted by

10. *See Gmail Usage per Country*, APPAPPEAL, https://web.archive.org/web/20131201122639/http://www.appappeal.com/maps/gmail (last updated Nov. 30, 2013, 10:27 PM GMT) (accessed via the Internet Archive index).

11. *See, e.g.*, *Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations/index.html (last visited Jan. 28, 2015).

12. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990).

13. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 155 (2004) (allowing U.S. agents to disassemble the gas tank of a car that was crossing the border without requiring reasonable suspicion or probable cause).

14. *See In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008).

15. *See generally* EDWARD LUCAS, THE SNOWDEN OPERATION: INSIDE THE WEST'S GREATEST INTELLIGENCE DISASTER (2014).

16. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://wapo.st/1ergqvs (discussing how the NSA intercepts the "buddy lists" of Internet users outside the United States with no judicial oversight).

17. *See* Defendant's Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act & Motion for Discovery at 2, United States v. Muhtorov, No. 12-cr-00033-JLK-1 (D. Colo. Jan. 29, 2014), *available at* https://www.aclu.org/sites/default/files/assets/muhtorov_-_defendants_motion_to_suppress.pdf.

the U.S. government.[18] Muhtorov's motion to suppress raises a host of novel extraterritorial issues: Who has Fourth Amendment rights, based on communications intercepted where, and when communicating with whom?

This Article considers the clash between the territorial Fourth Amendment and the global Internet. It asks how Fourth Amendment law should adapt to the reality of a global network in which suspects, victims, and evidence might be located anywhere. Specifically, this Article raises two sets of questions and then proposes answers to them. The first set of questions considers who has Fourth Amendment rights over the global Internet and the consequences this has for Internet surveillance law. The second set considers how the reasonableness requirement of the Fourth Amendment applies over the global Internet.

The first set of questions grapples with the Supreme Court's decision in *United States v. Verdugo-Urquidez*, which held that a person must have sufficient voluntary connections to the United States to enjoy Fourth Amendment rights.[19] Under *Verdugo-Urquidez*, some people in the world have Fourth Amendment rights, and many others do not. The distinction creates three important puzzles to solve before applying the Fourth Amendment to the Internet. First, how should online contacts with the United States factor into whether a person has Fourth Amendment rights? Second, how does the Fourth Amendment apply when the government does not know if a target has sufficient contacts to establish Fourth Amendment rights? And third, how does the Fourth Amendment apply when the government monitors communications between those who lack Fourth Amendment rights and others who have those rights?

The second set of questions assumes that the subject of monitoring has Fourth Amendment rights and considers how Fourth Amendment reasonableness varies depending on where a search occurs. The Supreme Court has held that the government has very broad power to search at the international border.[20] In addition, circuit courts have held that searches outside the United States are governed by standards of reasonableness rather than the domestic standard of a warrant.[21] These location-based distinctions raise three difficult questions that must be answered to apply the Fourth Amendment over the global Internet. First, how does the border search exception apply to Internet transmissions that cross the international border? Second, should standards of reasonableness over the global Internet be keyed to the location of the person monitored or the location where the data is located? And third, if the government seizes data first and then searches it later, should the reasonableness standard follow the jurisdiction where the seizure occurred or where the search occurred?

The conflict between the territorial Fourth Amendment and the facts of the global Internet raise the prospect that the Internet will destabilize Fourth

---

18. *See id.* at 2-5, 54.
19. 494 U.S. 259, 274-75 (1990).
20. *See infra* Part I.B.
21. *See infra* Part I.C-D.

Amendment law. Perhaps the global Internet will minimize the role of the Fourth Amendment, giving the government easy ways to circumvent constitutional protections. On the other hand, the Internet might expand Fourth Amendment protections, restricting the government far more than before. This Article follows an interpretive approach, "equilibrium-adjustment,"[22] that rejects these extremes. The theory of equilibrium-adjustment aims to maintain the role of the Fourth Amendment as changing technology and social practice threaten to alter the function of preexisting Fourth Amendment rules.[23] When changing technology substantially expands or restricts government power based on preexisting doctrine, courts can adjust constitutional protection to maintain the role of the Fourth Amendment over time.[24] Applying this methodology to the Internet requires seeking a way to retain the existing role of constitutional protection in limiting police power and avoiding dramatic shifts in police power over the transition from territorial to global facts.

This Article proposes the following answers to the two categories of questions. For the first category, it begins by concluding that online contacts should not create Fourth Amendment protection under *Verdugo-Urquidez*. The Fourth Amendment should apply only when a person monitored has sufficient physical or legal contacts with the United States. Next, when the government does not know if a person monitored has Fourth Amendment rights, such monitoring should be deemed constitutional as long as investigators had a reasonable, good faith belief that their conduct complied with the Fourth Amendment. Finally, when a person with Fourth Amendment rights communicates with another who lacks Fourth Amendment rights, the government must fully satisfy the Fourth Amendment standards for monitoring the person with Fourth Amendment rights.

This Article also proposes answers to the second set of questions about the reasonableness standard for global searches. First, it argues that the border search exception should not apply to purely electronic transmissions. The border search exception should be limited to physical and tangible property; it should not apply to allow scanning of electronic transmissions that cannot impact what crosses the border. Second, standards of reasonableness should be keyed to the location of the government's search or seizure rather than the location of individuals with Fourth Amendment rights in the communication. Finally, when the government seizes data first and then searches it later at a different location, the reasonableness standard should follow the rules of the jurisdiction where the data was initially seized.

---

22. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

23. *See id.* at 480-81.

24. *See id.* at 487-89.

This Article does not attempt to resolve every Fourth Amendment issue prompted by global computer networks.[25] Instead, it is intended to offer a general framework for applying the Fourth Amendment to a global computer network in a way that maintains the existing territorial conception of the Fourth Amendment. The global Internet threatens to dramatically destabilize Fourth Amendment law by disassociating person, place, and data. The rules offered in this Article can preserve the role of the Fourth Amendment by blocking its evisceration while at the same time maintaining its fundamental balance. These rules protect the role of the Fourth Amendment as we translate it not only from a physical to a networked world but also from a local investigative environment to a global one.

This Article proceeds in three Parts. Part I identifies the existing case law that has established the basic territorial principles of the Fourth Amendment. Part II considers and answers the new questions raised by the application of *Verdugo-Urquidez* to the Internet. Part III considers and answers the new questions raised by a territorially based reasonableness standard.

I. THE TERRITORIAL FOURTH AMENDMENT

Appreciating the clash between the global Internet and the territorial Fourth Amendment requires an understanding of how existing doctrine applies beyond U.S. borders. Although existing law remains sparse, it consistently reflects what we might term a "territorial" conception of the Fourth Amendment. To be clear, this does not mean that the Fourth Amendment has no application outside U.S. borders. Rather, it signals that protection varies depending on the connection between the search or seizure and the territory of the United States.

Because courts will use existing doctrine to frame how the Fourth Amendment applies to the Internet, it helps to begin with existing case law on the territorial Fourth Amendment. Existing decisions on the territorial Fourth Amendment have addressed three basic questions. First, who is entitled to Fourth Amendment protection? Second, how does the Fourth Amendment apply at the international border? And third, what protection applies to searches abroad? This Part will address each in turn.

A. *Who Is Entitled to Fourth Amendment Protection?*

The leading case on the territorial Fourth Amendment is the Supreme Court's decision in *United States v. Verdugo-Urquidez*.[26] Under *Verdugo-*

25. Important matters left unaddressed include the proper reasonableness standard courts should adopt for extraterritorial searches and precisely how much contact with the United States should be required to establish Fourth Amendment rights. This Article assumes that such questions will be answered elsewhere, and it focuses instead on questions raised by applying that law to Internet communications.

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

Urquidez, the Fourth Amendment is implicated only when a subject of monitoring has contacts with the United States because of either lawful presence in the United States at the time of the search or some substantial connection such as citizenship or lawful residency.

Verdugo-Urquidez involved a search of two houses in Mexico owned by a Mexican drug kingpin.[27] U.S. law enforcement officials believed that the searches would prove the defendant's involvement in a massive drug trafficking conspiracy as well as the murder of a U.S. agent.[28] By the time of the search, the defendant had already been arrested in Mexico and transported to San Diego to face charges in federal court.[29] The defendant later moved to suppress the evidence from the searches of his Mexican properties on the ground that the searches violated his Fourth Amendment rights.[30]

The Court ruled in an opinion by Chief Justice Rehnquist that the defendant could not invoke the Fourth Amendment.[31] The Fourth Amendment protects the "right of the people," Rehnquist reasoned, and references to "the people" in the Constitution signify a political community rather than the world at large: the term "refers to a 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."[32] That conclusion was bolstered by historical evidence showing "that the 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 of the United States territory."[33]

Because Verdugo-Urquidez was an alien with "no previous significant voluntary connection with the United States," he was not one of "the people" that the Fourth Amendment protects.[34] That was true even though he had been arrested and brought to the United States a few days before the search occurred in Mexico. A brief and involuntary presence was not a "substantial connection with our country" that could generate Fourth Amendment protection, as it was merely a "fortuitous circumstance" controlled by law enforcement authorities.[35]

Justice Kennedy provided the fifth vote for the majority and also authored a concurring opinion.[36] Notably, Justice Kennedy's concurring opinion offered

27. *See id.* at 262.
28. *Id.*
29. *See id.*
30. *See id.* at 263.
31. *See id.* at 274-75.
32. *Id.* at 265 (quoting U.S. CONST. amend. IV).
33. *Id.* at 266.
34. *Id.* at 271-72.
35. *Id*.
36. *See id.* at 261.

a different rationale than the majority opinion he joined. Justice Kennedy rejected reliance on "the people" as relevant to the Fourth Amendment's reach, and instead he offered a pragmatic argument about why the defendant's Fourth Amendment rights had not been violated. Verdugo-Urquidez had challenged the absence of a U.S. warrant to search his home, but a warrant requirement abroad was infeasible:

> The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country.[37]

Verdugo-Urquidez is difficult to interpret for two primary reasons. First, there is some uncertainty about whether Chief Justice Rehnquist's opinion or Justice Kennedy's concurrence acts as the binding opinion.[38] On one hand, Rehnquist's opinion was announced as the opinion of the Court. Under a traditional doctrinal approach, it should be the binding decision.[39] On the other hand, Justice Kennedy's view was recently echoed by the Court majority in the context of the Suspension Clause in *Boumediene v. Bush*,[40] creating at least a plausible argument that Justice Kennedy's approach applies in the Fourth Amendment setting as well.[41]

Verdugo-Urquidez also remains difficult to interpret because its vague language has been interpreted in only a few lower court decisions that themselves are not models of clarity. Consider the question of whether a regular visitor to the United States develops Fourth Amendment rights. In *American Immigration Lawyers Ass'n v. Reno*,[42] a district court suggested that the answer is no. The court, in the context of a Fifth Amendment due process claim, held that a person who regularly came to the United States to visit her daughter and grandchild did not have sufficient connections to the United States to satisfy the *Ver-*

---

37. *Id.* at 278 (Kennedy, J., concurring).

38. *See, e.g.*, Hernandez v. United States, 757 F.3d 249, 265 (5th Cir.) (concluding that Chief Justice Rehnquist's opinion is binding), *reh'g en banc granted*, 771 F.3d 818 (5th Cir. 2014); United States v. Stokes, 710 F. Supp. 2d 689, 698-700 (N.D. Ill. 2009), *aff'd*, 726 F.3d 880 (7th Cir.), *cert. denied*, 134 S. Ct. 713 (2013); United States v. Esparza-Mendoza, 265 F. Supp. 2d 1254, 1260-61 (D. Utah 2003) (concluding that the "court is not at liberty to second-guess Justice Kennedy's direct statement that he was joining the Court's opinion"), *aff'd*, 386 F.3d 953 (10th Cir. 2004); United States v. Guitterez, 983 F. Supp. 905, 912 (N.D. Cal. 1998) (categorizing Chief Justice Rehnquist's opinion as a plurality opinion), *rev'd on other grounds*, 203 F.3d 833 (9th Cir. 1999).

39. *See Hernandez*, 757 F.3d at 265.

40. 553 U.S. 723, 764 (2008) (concluding that "questions of extraterritoriality turn on objective factors and practical concerns, not formalism"); *id.* at 759-60 (citing Justice Kennedy's concurrence in *Verdugo-Urquidez*).

41. For example, in *Hernandez*, the Fifth Circuit concluded that the proper test, applied "in light of *Boumediene*'s general functional approach," was Chief Justice Rehnquist's majority opinion in *Verdugo-Urquidez*. 757 F.3d at 266 (italics omitted).

42. 18 F. Supp. 2d 38 (D.D.C. 1998), *aff'd*, 199 F.3d 1352 (D.C. Cir. 2000).

dugo-Urquidez standard.[43] On the other hand, in *Martinez-Aguero v. Gonzalez*,[44] the Fifth Circuit suggested that the answer is yes. A Mexican woman with an expired visitor's visa went to the U.S. consular office and applied for a new visa.[45] The officials stamped her expired visa and told her she could continue to rely on the expired one until a new visa arrived.[46] The woman came to the United States for her monthly visit with her aunt and was stopped on the U.S. side of the Texas-Mexico border.[47] The Fifth Circuit held that the woman's regular visits and reliance on the consular office established sufficient contacts with the United States to have Fourth Amendment rights.[48]

Next consider a pair of opinions by then-Judge Cassell on whether illegal aliens inside the United States have Fourth Amendment rights. In *United States v. Esparza-Mendoza*, Judge Cassell ruled that an illegal alien who had previously been deported for committing a felony cannot establish Fourth Amendment rights inside the United States.[49] On the other hand, two years later, in *United States v. Atienzo*, Judge Cassell ruled that the same rule did not necessarily apply to illegal aliens who had not been previously deported for committing a felony.[50] The "multitudinous fact patterns" that could arise with aliens who had not been previously deported for felonies presented "complexities" that "may not always be susceptible to categorical analysis" and instead required a "case-by-case determination."[51] In other words, there was no clear answer to the important question of whether and when illegal aliens inside the United States have Fourth Amendment rights.

B. *The Fourth Amendment at the International Border*

The next territorial limit on the Fourth Amendment involves its application at the international border. The Supreme Court has held that a border search exception to the Fourth Amendment applies to property entering and exiting the United States at the border, as well as its functional equivalent,[52] in order to protect the sovereign interests of the United States in monitoring what enters

43. *Id.* at 59, 60 & n.17.

44. 459 F.3d 618 (5th Cir. 2006).

45. *Id.* at 620.

46. *Id.*

47. *See id.*

48. *See id.* at 625.

49. 265 F. Supp. 2d 1254, 1271 (D. Utah 2003), *aff'd on other grounds*, 386 F.3d 953 (10th Cir. 2004).

50. No. 2:04-CR-00534 PGC, 2005 WL 3334758, at *1 (D. Utah Dec. 7, 2005).

51. *Id.* at *4-5.

52. *See* Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973) ("Whatever the permissible scope of intrusiveness of a routine border search might be, searches of this kind may in certain circumstances take place not only at the border itself, but at its functional equivalents as well.").

and exits the country.[53] In most cases, searches at the border are always permitted even without reasonable suspicion.[54] At the same time, the Supreme Court has left open the possibility (pursued by the Ninth Circuit) that some particularly invasive searches require justification.[55] As a result of the border search doctrine, the Fourth Amendment applies very differently at the border than elsewhere—and it usually provides no protections at all.

Two lines of cases are particularly helpful to understand how the border search exception might apply to Internet communications. First, the Fourth and Ninth Circuits have applied the border search exception to the search of a personal computer physically crossing the border.[56] For example, in *United States v. Ickes*, customs agents stopped the defendant's van at the Canadian border.[57] After observing the defendant's suspicious behavior, the agents searched the van and seized a computer and several dozen storage disks.[58] A search of the computer and disks uncovered child pornography.[59] The Fourth Circuit held that the agents had lawfully searched the computers and disks because they had been brought to the border.[60] No reasonable suspicion was required: the border search doctrine allowed a search through the computer just as it allowed a search of other physical property. The court rejected the defendant's argument that the border search doctrine should apply differently to computer searches because computers store expressive material: "Following Ickes's logic would create a sanctuary at the border for all expressive material—even for terrorist plans. This would undermine the compelling reasons that lie at the very heart of the border search doctrine."[61]

The Ninth Circuit recently added a caveat to this doctrine for searches using forensic software. In *United States v. Cotterman*, agents seized a suspect's laptop computer at the border and then had a forensic specialist examine it using computer forensic software that revealed contraband images.[62] Sitting en

---

53. *See* United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004).

54. *See, e.g.*, *id.*

55. In *United States v. Montoya de Hernandez*, the Court indicated that a balancing test may be appropriate and that in certain circumstances a higher level of suspicion may be required to justify a nonroutine border search. *See* 473 U.S. 531, 539-40 (1985). Accordingly, the Ninth Circuit has imposed a reasonable suspicion requirement on searches deemed nonroutine. *See, e.g.*, United States v. Cotterman, 709 F.3d 952, 962-64 (9th Cir. 2013) (en banc) (contrasting a forensic examination at the border, which "directly implicat[es] substantial personal privacy interests" and therefore requires reasonable suspicion, with a "routine border search" for which no suspicion is required (quoting *Montoya de Hernandez*, 473 U.S. at 540) (internal quotation mark omitted)).

56. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1007-08 (9th Cir. 2008); United States v. Ickes, 393 F.3d 501, 506-08 (4th Cir. 2005).

57. 393 F.3d at 502.

58. *Id.* at 502-03.

59. *Id.* at 503.

60. *See id.* at 506-08.

61. *Id*. at 506.

62. 709 F.3d 952, 956-58 (9th Cir. 2013) (en banc).

banc, the Ninth Circuit ruled that the Fourth Amendment required reasonable suspicion to search a computer using sophisticated forensic software. The court reasoned that forensic searches are akin to "computer strip search[es]."[63] Under the Ninth Circuit's rule, manual analysis of a computer seized at the border requires no justification, but forensic analysis requires reasonable suspicion.[64]

The second line of cases has applied the border search exception to allow opening and reading international mail at the border or its functional equivalent without reasonable suspicion.[65] For example, in *United States v. Seljan*, customs inspectors looking for currency violations opened Seljan's FedEx packages sent through a routing center in Oakland, California, before being shipped overseas.[66] The inspectors found sexually suggestive letters indicating that Seljan was going to travel to the Philippines to engage in sex with minors.[67] The en banc Ninth Circuit held that the Fourth Amendment permitted the agents to open Seljan's packages and visually scan his letters at the FedEx facility.[68] Investigators did not destroy property or conduct an invasive search of Seljan's person, the court reasoned, and the initial letter came into plain view when the package was opened.[69] The search was reasonable because the incriminating nature of the letter was immediately apparent upon a quick scan, and the agent did nothing more than scan the letter in a reasonable way related to his statutory duty to investigate customs offenses.[70]

The cases allowing searches of physical computers and the opening and reading of international mail at the border suggest a potentially broad (if not limitless) power at the border or its virtual equivalent to read the contents of electronic communications. At the same time, no court has yet addressed whether the border search exception also allows the interception of purely electronic transmission.

---

63. *Id.* at 966. Whether the Supreme Court would accept this doctrine remains unclear.

64. The distinction between forensic and manual analysis is hardly clear. For a discussion, see Orin Kerr, *What Is the Ninth Circuit's Standard for Border Searches Under* United States v. Cotterman*?*, VOLOKH CONSPIRACY (March 11, 2013, 3:12 PM), http://www.volokh.com/2013/03/11/what-is-the-ninth-circuits-standard-for-border-searches-under-united-states-v-cotterman.

65. *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 611-13, 622 (1977) (upholding a federal statute that allowed customs officials to read international mail under a "reasonable cause to suspect" standard, which the Court defined as "a practical test which imposes a less stringent requirement than that of 'probable cause' imposed by the Fourth Amendment" (quoting 19 U.S.C. § 482)).

66. 547 F.3d 993, 996 (9th Cir. 2008) (en banc).

67. *Id.* at 996-97.

68. *Id.* at 1008.

69. *See id.* at 1002, 1005.

70. *Id.* at 1005; *see also* United States v. Glasser, 750 F.2d 1197, 1203 (3d Cir. 1984) (collecting circuit court cases upholding searches of incoming and outgoing international mail without a warrant or probable cause); United States v. Richards, 638 F.2d 765, 773 (5th Cir. Mar. 1981) (allowing the search of already-delivered international packages under the extended border search exception subject to certain limitations).

C. *Reasonableness Abroad*

The next question is how the Fourth Amendment reasonableness requirement applies to searches outside the United States. Three circuit courts have addressed the question so far, with two distinct approaches emerging. The Ninth Circuit has held that when the U.S. government cooperates with foreign authorities to conduct a search or seizure abroad, Fourth Amendment reasonableness requires investigators to comply with foreign law in the jurisdiction where the search occurs.[71] On the other hand, the Second and Seventh Circuits have held that when the United States is involved in an extraterritorial search, either acting alone or through a joint investigation with foreign governments,[72] Fourth Amendment reasonableness requires a balancing of the government need and the privacy interest but does not require a warrant.

1. *The Ninth Circuit standard*

The first decision on how the reasonableness standard applies to foreign searches was the Ninth Circuit's decision in *United States v. Peterson*, authored by then-Judge (now-Justice) Anthony Kennedy. In *Peterson*, the Drug Enforcement Agency (DEA) was investigating a massive scheme to transport marijuana by ship from Thailand to the Philippines and then on to the United States.[73] The DEA tipped off law enforcement in the Philippines and told them about a suspected conspirator who lived in a Manila apartment.[74] The local authorities wiretapped the apartment's radio transmitter without a warrant, and the wiretap revealed the location of the ship; a subsequent search of the ship uncovered marijuana.[75] The defendant who was wiretapped then sought suppression of the marijuana on the ground that the warrantless wiretap violated his Fourth Amendment rights.[76]

Judge Kennedy reasoned that the wiretap was the product of a joint investigation between the DEA and authorities in the Philippines and that the constitutional reasonableness of the search depended on its compliance with Philippine law.[77] The Ninth Circuit had sought supplemental briefing on this

---

71. *See* United States v. Peterson, 812 F.2d 486, 490 (9th Cir. 1987).

72. Under Second Circuit precedent, the Fourth Amendment may apply when either (1) the United States acts alone or (2) a foreign government acts either as an agent of the United States or in cooperation with the United States in an attempt to circumvent protections that would apply to U.S. officials. *See* United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992). The foreign government must be acting as a genuine agent of the United States: a joint investigation in which both sovereigns are pursuing the same goal does not automatically trigger that standard. *See* United States v. Lee, 723 F.3d 134, 140-41 (2d Cir. 2013).

73. *Peterson*, 812 F.2d at 488-89.

74. *Id.* at 488.

75. *Id.* at 488-89.

76. *Id.* at 489.

77. *See id.* at 490.

question, and Judge Kennedy's opinion provides a thorough discussion of the relevant principles and precedents under Philippine law, ranging from the Philippine Constitution[78] to Philippine statutes,[79] judicial precedents,[80] and even a Philippine law review article.[81] Judge Kennedy concluded that the lawfulness of the monitoring posed a difficult question of Philippine law and that it was plausible that a warrant was required and that the wiretap was illegal. If so, the Fourth Amendment was violated.[82]

Judge Kennedy then reasoned that even if the warrantless surveillance violated the Fourth Amendment, the remedy remained an issue of U.S. law: "Although local law of the Philippines governs whether the search was reasonable, our law governs whether illegally obtained evidence should be excluded . . . ."[83] For this, Judge Kennedy adopted a broad view of the then-nascent good faith exception to the exclusionary rule[84]: so long as "law enforcement officers acted on a reasonable belief that their conduct was legal," the good faith exception applied.[85] This was "a rational accommodation to the exigencies of foreign investigations," Judge Kennedy reasoned, given that U.S. officials are "not in an advantageous position to judge whether the [foreign] search was lawful."[86]

Peterson's adoption of foreign law as the standard of reasonableness has been followed by lower courts in cases involving joint investigations between U.S. and foreign authorities since its debut in 1987, in the case of both physical searches and wiretaps.[87] At one level, the framework is puzzling: it allows stat-

78. *See id.* at 491 (citing CONST. (1973), art. IV, sec. 4 (Phil.)).

79. *See id.* (citing An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purposes, Rep. Act No. 4200, §§ 1, 3, 20 LAWS & RES. 50, 50-51 (June 19, 1965) (Phil.)).

80. *See id.* (citing Marcelo v. de Guzman, G.R. No. L-29077, 114 S.C.R.A. 657 (June 29, 1982) (Phil.)).

81. *See id.* (citing Tristan A. Catindig, Comment, *The Wire Tapping Law and Its Constitutional Implications*, 41 PHIL. L.J. 352 (1966)).

82. *See id.*

83. *Id.*

84. *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.3, at 67-71 (5th ed. 2012) (discussing the introduction of the good faith exception to the exclusionary rule).

85. *Peterson*, 812 F.2d at 492.

86. *Id.*

87. The Ninth Circuit reaffirmed the joint venture framework in *United States v. Barona*, which held that the lower court's finding that a wiretap of the defendants by Danish authorities was a joint investigation was not clearly erroneous and that the wiretap was therefore governed by Danish law. 56 F.3d 1087, 1096 (9th Cir. 1995). In addition, the framework has been applied by several district courts. *See, e.g.*, United States v. Rosenau, No. CR06-157MJP, 2011 WL 4957357, at *2 (W.D. Wash. Oct. 18, 2011) (concluding that the exclusionary rule would not apply even if the search were a joint venture because no facts indicated it was unreasonable for U.S. authorities to rely on the assurances of Canadian law enforcement officers that the search complied with Canadian law); Lau v. United States, 778 F. Supp. 98, 101 (D.P.R. 1991) (finding the assurance of the Attorney General for the Neth-

utory protections abroad to create constitutional rights in the United States and may even allow conduct that would not be a search or seizure in the United States to amount to a search or seizure if conducted abroad. But when limited to joint investigations, the approach has a commonsense quality. When U.S. investigators work together with their foreign counterparts to conduct a foreign search, foreign court orders often must be obtained. Cooperating with foreign governments and following their domestic law complies with the legal standard recognized where the search occurs. From this perspective, reasonableness reflects a norm of cooperation among the different governments interested in investigating the case.

2. *The Second and Seventh Circuit standard*

The second approach to extraterritorial reasonableness is the general balancing standard adopted by the Second and Seventh Circuits. The first case to adopt this standard was the Second Circuit's decision in *In re Terrorist Bombings of U.S. Embassies in East Africa*.[88] In 1996, American intelligence authorities began tapping the telephone lines of a suspected al Qaeda cell in Kenya.[89] In 1997, American and Kenyan authorities raided the home of one of the suspects, Wadih El-Hage, who happened to be a U.S. citizen and therefore had Fourth Amendment rights. No U.S. warrant was obtained, but investigators had what purported to be a Kenyan search warrant.[90] El-Hage eventually was charged with offenses in the United States based in part on the fruits of the wiretapping and physical search in Kenya.[91]

In an opinion authored by Judge Cabranes, the Second Circuit ruled that the monitoring did not violate the Fourth Amendment. The court ruled that the warrant requirement of the Fourth Amendment does not apply to searches that occur outside the United States.[92] When a search occurs abroad, the court concluded, the Fourth Amendment requires reasonableness but not a warrant. Judge Cabranes noted that U.S. warrants for extraterritorial searches were essentially unknown and were of no obvious force abroad; it was not even clear that U.S. officials had the legal authority to issue such warrants.[93] Given these practical problems, the court concluded, the warrant requirement did not extend overseas.

---

erlands Antilles that no search and seizure warrant was required under Dutch law sufficient to admit evidence); United States v. Scarfo, No. 88-00003-1-19, 1988 WL 115805, at *4 (E.D. Pa. Oct. 26, 1988) (concluding that even if there were a joint venture, the exclusionary rule would not apply because of the U.S. officials' good faith belief that their conduct complied with foreign law).

88. 552 F.3d 157, 167 (2d Cir. 2008).

89. *See id.* at 159.

90. *Id.* at 159-60.

91. *See id.* at 159.

92. *Id.* at 171.

93. *Id.*

Next, the court held that constitutional reasonableness must be judged by weighing the government interests justifying the search against the severity of the privacy invasion of the suspect's Fourth Amendment rights.[94] In El-Hage's case, "the searches' intrusion on El-Hage's privacy was outweighed by the government's manifest need to monitor his activities as an operative of al Qaeda because of the extreme threat al Qaeda presented, and continues to present, to national security."[95] The search of his home occurred in daylight and was not covert; the search had been personally authorized by the U.S. Attorney General and was in furtherance of an extremely important investigation into a serious threat.[96] The wiretaps were reasonable even though they were extremely invasive because "the surveillance of suspected al Qaeda operatives must be sustained and thorough in order to be effective."[97] "While the intrusion on El-Hage's privacy was great," Judge Cabranes reasoned, "the need for the government to so intrude was even greater."[98]

The Seventh Circuit largely adopted the Second Circuit's approach in a recent decision, *United States v. Stokes*.[99] In *Stokes*, a U.S. citizen moved to Thailand and molested children there.[100] U.S. and Thai government officials worked together to obtain a Thai warrant to search his home in Thailand; the search revealed thousands of images of child pornography on the suspect's home computer.[101] Stokes was extradited to the United States, where he was convicted of traveling in foreign commerce for the purpose of engaging in a sex act with a minor.[102] Stokes moved to suppress the evidence from his home in Thailand.[103]

In a decision by Judge Sykes, the Seventh Circuit agreed with the Second Circuit that the Fourth Amendment warrant requirement did not apply outside the United States.[104] The Seventh Circuit then applied a general reasonableness standard, mirroring the balancing approach adopted by the Second Circuit but applying it in a criminal case. The search was reasonable, the court held, because of "the government's strong interest in preventing the sexual exploitation of children"[105] and the overall reasonableness of the search: although it occurred in the defendant's home, there was probable cause to believe evidence of a crime was in the home, the Thai government had obtained a valid Thai

94. *See id.* at 176.
95. *Id*. at 172-73.
96. *Id.* at 173-74.
97. *Id.* at 176.
98. *Id.*
99. 726 F.3d 880 (7th Cir.), *cert. denied*, 134 S. Ct. 713 (2013).
100. *Id.* at 885-86.
101. *Id.* at 886.
102. *Id.* at 886-87.
103. *Id.* at 887.
104. *Id.* at 885 ("Following the Second Circuit, we hold that the Fourth Amendment's warrant requirement and the Warrant Clause have no extraterritorial application.").
105. *Id.* at 893.

warrant, and the search was executed in a way that minimized its intrusiveness.[106]

Although they differ in some ways, it is possible to reconcile the Second and Seventh Circuits' no-warrant general reasonableness standard with the Ninth Circuit's foreign-law good faith standard. The two standards are different in their particulars, certainly. The Ninth Circuit standard is more rule-like and clear; the Second and Seventh Circuit standard is more standard-like and amorphous. At the same time, the two standards can be reconciled in part. If a foreign search warrant is not a search warrant for Fourth Amendment purposes, then a foreign search in reliance on foreign law (the Ninth Circuit approach) does not require a warrant (the Second and Seventh Circuit approach). And if compliance with foreign law is a factor in the reasonableness inquiry, as *Stokes* suggests, then the two standards will often produce the same results in practice.

D. *The Territorial Fourth Amendment and Equilibrium-Adjustment*

As the preceding discussion shows, territoriality is critical to Fourth Amendment protection outside the United States. Only persons with sufficient contacts with the United States have Fourth Amendment rights; those who have Fourth Amendment rights can lose many or all of those rights at the border; and once they leave the United States, their Fourth Amendment rights morph from the usual domestic warrant requirement to some form of reasonableness balancing.

This Article accepts the basic principles of existing doctrine and considers how courts should apply those principles in light of the unprecedented globalism of today's Internet. When courts consider how the Fourth Amendment applies to the Internet, they will do so with the principles of existing law as a backdrop. But applying those principles to the global Internet raises many uncertainties and ambiguities, and a theory is needed to resolve them.

This Article uses the theory of equilibrium-adjustment to provide those answers.[107] Equilibrium-adjustment focuses on how technology changes the significance of prior Fourth Amendment rules. When changing technology and social practice threaten a major change in the balance of government power under then-existing law, the application of equilibrium-adjustment aims to settle ambiguities or adopt new rules that restore the function of the rules before the technological change.[108] Equilibrium-adjustment recognizes that new technologies can change the balance between government power and civil liberties struck in an earlier age, and it allows courts to adopt rules in light of technological change to restore or maintain that balance.[109]

---

106. *Id.* at 893-94.

107. *See generally* Kerr, *supra* note 22.

108. *Id.* at 487-88.

109. *Id.*

Fourth Amendment case law often reflects equilibrium-adjustment,[110] and the Supreme Court's recent opinion in *Riley v. California*[111] offers a useful demonstration of the method. In 1973, the Supreme Court held in *United States v. Robinson* that the police can always conduct a complete search of a person on arrest.[112] Forty-one years later, in *Riley*, the Court was asked to decide whether *Robinson* also allows police to search a cell phone that an arrestee had in his possession at the time of arrest. *Riley* held that it does not: although agents can conduct a complete search of physical evidence on a person under *Robinson*, searching a cell phone requires a warrant.[113] The Court reasoned that searching a cell phone is much more invasive than searching physical evidence a person might carry with him.[114] Physical searches of items on a person tend to be narrow, as most people can only carry so many letters, pictures, or books.[115] On the other hand, cell phones have an immense storage capacity and often store very sensitive information.[116]

Riley provides a helpful example of equilibrium-adjustment. In 1973, a rule authorizing a complete search of the property on an arrested person meant one thing. By 2014, it meant something else. Changing technology and social practice transformed the significance of *Robinson*'s rule. To avoid a dramatic expansion of government power based on facts that could not have been imagined when the prior rule was announced, *Riley* carved out an exception to *Robinson*'s permissive rule for cell phones (and, implicitly, other electronic storage devices). *Riley* maintains the balance of power struck before the digital age by excepting digital devices from the preexisting rule. Adjusting the constitutional rule for new facts maintains the equilibrium of the prior doctrine.

II. *VERDUGO-URQUIDEZ* AND THE GLOBAL INTERNET

When courts apply the Fourth Amendment in the typical domestic context, they can safely assume that every defendant has Fourth Amendment rights. Fourth Amendment analysis focuses instead on searches and seizures, reasonableness, and remedies for violations. Under *United States v. Verdugo-Urquidez*, however, that assumption is no longer automatic when applying the Fourth Amendment to the Internet.[117] The threshold question of whether the person monitored has any Fourth Amendment rights takes on new importance. The precise standard adopted by *Verdugo-Urquidez* remains murky, and this Part

110. *See id.* at 495-525.

111. 134 S. Ct. 2473 (2014).

112. 414 U.S. 218, 235 (1973).

113. *Riley*, 134 S. Ct. at 2495 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

114. *See id*. at 2489-91.

115. *See id*. at 2489.

116. *See id.* at 2489-91.

117. *See* 494 U.S. 259, 265-66 (1990).

does not attempt to answer every aspect of it. Instead, it considers three Internet-specific questions prompted by *Verdugo-Urquidez* that courts will have to answer to apply the Fourth Amendment in global Internet cases.

First, are online contacts relevant to the *Verdugo-Urquidez* inquiry? Users outside the United States can easily take advantage of U.S.-based Internet services. They might store files in "the cloud" on U.S.-based servers, visit U.S. websites, read and post to U.S. blogs, and live online lives identical to U.S. citizens inside the United States. Can those online contacts create Fourth Amendment rights—or at least help create them?

Second, how should the Fourth Amendment apply if the government mistakenly believes that a subject of monitoring lacks Fourth Amendment rights? Internet surveillance over global networks makes common a previously rare situation: investigators may not know whether the suspect monitored has Fourth Amendment rights under *Verdugo-Urquidez*. In the online setting, investigators usually begin investigating a crime without knowing who is behind it. This raises an important question of how the Fourth Amendment applies when a target's "*Verdugo-Urquidez* status" is unknown. And specifically, how does the law apply when investigators believe a suspect lacks Fourth Amendment rights, conduct monitoring, and later realize their belief was erroneous?

Third, how should the Fourth Amendment apply when the government monitors communications between persons with Fourth Amendment rights under *Verdugo-Urquidez* and those who lack those rights? When a communication is in transit, the usual Fourth Amendment rule is that both the sender and receiver have a reasonable expectation of privacy in its contents.[118] *Verdugo-Urquidez* adds an additional wrinkle: the government might monitor communications between one person with Fourth Amendment rights and another who lacks those rights. Does the Fourth Amendment not apply because the government can monitor the party who lacks Fourth Amendment rights, or does the Fourth Amendment continue to apply because one party has those rights?

This Part offers the following proposed answers. First, online contacts with the United States should be irrelevant to the *Verdugo-Urquidez* inquiry. Fourth Amendment rights should be generated by physical contacts or a legal relationship with the United States, not virtual contacts. Two arguments support that conclusion. As a matter of doctrine, it appears most consistent with the reasoning in *Verdugo-Urquidez*. And as a matter of policy, such a conclusion is necessary to maintain the role of the Fourth Amendment in a networked world. Internet technologies destabilize the *Verdugo-Urquidez* inquiry by disrupting the prior relationship between person and place. Recognizing that online contacts cannot establish rights is necessary to retain the territorial Fourth Amendment.

Second, when a suspect's *Verdugo-Urquidez* status is uncertain, the Fourth Amendment requires a reasonable, good faith belief that the monitoring complied with the Fourth Amendment. If the government monitors a suspect based

118. *See generally* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE §§ 4.1-.4 (3d ed. 2000).

on the belief that the suspect lacks Fourth Amendment rights, but that belief is later proven false, the monitoring should be deemed unconstitutional only if the belief was unreasonable. Where a belief that a suspect lacked *Verdugo-Urquidez* rights is reasonable, the officer's misunderstanding is regrettable but not culpable; the Fourth Amendment requires reasonableness, not perfection. By analogy to the apparent authority doctrine of *Illinois v. Rodriguez*,[119] a reasonable, good faith belief that a suspect lacks Fourth Amendment rights should render the government's search constitutionally reasonable.

Third, the Fourth Amendment should continue to apply when the government monitors a communication between one party who has Fourth Amendment rights and a second party who lacks Fourth Amendment rights. The *Verdugo-Urquidez* inquiry acts as an additional question of whether the Fourth Amendment applies apart from whether a search or seizure occurred. As a result, if one person monitored has Fourth Amendment rights, the government must fully respect those rights. Any other approach would offend the principles of equilibrium-adjustment by unduly limiting Fourth Amendment protection based on the fortuity of where a party to a communication may be located.

A. *Should Online Contacts Establish Fourth Amendment Rights?*

The first question is whether online contacts factor into the *Verdugo-Urquidez* inquiry. Contacts with a sovereign can be legal relationships, such as citizenship. Contacts also can be physical, such as presence inside the borders. But contacts may also be virtual contacts established over the Internet. That possibility raises a question: If a noncitizen outside the United States uses U.S.-based Internet services to create a U.S.-based virtual life, do those contacts count for purposes of establishing Fourth Amendment rights under *Verdugo-Urquidez*? The answer should be no, for both doctrinal and functional reasons.

The first reason to reject virtual contacts as a basis for establishing Fourth Amendment rights is based on the reasoning of *Verdugo-Urquidez*. The majority opinion concluded that "the people" protected by the Fourth Amendment are those who are part of the political community that helped create and ratify the Constitution and who therefore can draw protection from it.[120] According to Chief Justice Rehnquist, "the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government."[121] He contrasted this with the possibility, "never suggested," that the Fourth Amendment "was intended to restrain the actions of the Federal Government against aliens outside of the United States territory" or "aliens in for-

119. 497 U.S. 177, 186 (1990) ("The Constitution is [not] violated when officers enter [a home] without a warrant because they reasonably (though erroneously) believe that the person who has consented to their entry is a resident of the premises . . . ."); *see infra* text accompanying notes 144-48.

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

121. *Id.* at 266.

eign territory or in international waters."[122] The Fourth Amendment applies to the former but not the latter.

Under the majority opinion, the fact that Verdugo-Urquidez had been arrested and brought to the United States to face charges a few days before the search of his Mexico home was irrelevant.[123] That contact with the United States was merely "the fortuitous circumstance of whether the custodian of its nonresident alien owner had or had not transported him to the United States at the time the search was made."[124] Because that "fortuitous circumstance" did not constitute a "previous significant voluntary connection with the United States," it could not establish Fourth Amendment rights.[125]

The reasoning of *Verdugo-Urquidez* indicates that online contacts should not establish Fourth Amendment rights. Online contacts with U.S. servers are merely the "fortuitous" circumstance of where the Internet provider happens to locate the servers. To an Internet user, the servers could be anywhere: the user generally does not know their location and does not care.[126] As a result, the fact that a server may be in the United States should not be a "significant voluntary connection" with the United States as a sovereign.

This is equally true if the contacts with the United States involve public debate and discussion rather than merely server use. The "community" in *Verdugo-Urquidez* is not a community of debaters or talking heads; rather, it is a community of individuals who rely on the Constitution as a countermajoritarian check on the government that rules over them. Foreigners who participate in online debates may influence U.S. opinion, and they may have an important role in influencing the conduct of U.S. officials. But influence does not bring one within the community of the governed in a constitutional system. The latter requires physical presence or at least the prospect of future physical presence or political participation. None of these can be generated by online contacts.

The same result can be reached under Justice Kennedy's concurring opinion, although that conclusion must be more tentative. Recall that Justice Kennedy rejected reliance on the concept of "the people" as defining the scope of Fourth Amendment law.[127] Instead, he looked to what rule was most consistent with the pragmatic role of the United States as a sovereign nation. According to Justice Kennedy, "we must interpret constitutional protections in light of the undoubted power of the United States to take actions to assert its legitimate

122. *Id.* at 266-67.

123. *See id.* at 271-72.

124. *Id.* at 272.

125. *Id.* at 271-72.

126. OFFICE OF TAX POLICY, DEP'T OF THE TREASURY, SELECTED TAX POLICY IMPLICATIONS OF GLOBAL ELECTRONIC COMMERCE § 7.2.3.1, at 25 (1996) ("Computer servers can be located anywhere in the world and their users are indifferent to their location.").

127. *Verdugo-Urquidez*, 494 U.S. at 276 (Kennedy, J., concurring).

power and authority abroad."[128] Justice Kennedy's framework does not lead to easy answers in part because the *Verdugo-Urquidez* inquiry poses only a threshold question. It is somewhat difficult to answer whether a particular person is entitled to any rights based on a standard that seems focused on whether a person has too many rights that could interfere with the function of a sovereign.

At the same time, the result I offer here is consistent with Justice Kennedy's method because it disallows foreign enemies of the United States from using online contacts to generate Fourth Amendment rights that could interfere with U.S. authority abroad. If any individual can generate Fourth Amendment rights solely by online contact, then foreign nationals and nation states seeking to do ill against the United States can thwart U.S. investigative and military powers by doing whatever it takes to generate those rights. The targets of U.S. military and surveillance power would have strong incentives to take those steps, as they could all be taken unilaterally: U.S. officials would have no effective way to stop them. As a result, a rule that online contacts can generate Fourth Amendment rights would interfere with U.S. power abroad in a way that would seem to conflict with Justice Kennedy's pragmatic vision.

An important caveat to that conclusion is that Justice Kennedy's opinion emphasizes the "legitimate power and authority" of the United States abroad.[129] There may be limits to what kind of power and authority counts as "legitimate" in Justice Kennedy's view. For example, Edward Snowden's leaks included reports that the NSA was widely monitoring foreign citizens rather than merely targeting foreign powers or individual terrorist suspects.[130] It is unclear if the allegations are true: the NSA vehemently denied them.[131] But whether or not the allegations are true, if the Fourth Amendment is read to allow such powers, it could be argued that such powers are "illegitimate" if abused or otherwise used in bad faith. Perhaps Justice Kennedy's conception of "legitimate" powers would apply, and perhaps it would not. Here, we must realistically acknowledge the limited usefulness of trying to pin down Justice Kennedy's precise meaning. Perhaps a sensible resolution is that his *Verdugo-Urquidez* concurrence can be read as supporting the view that online contacts do not generate Fourth Amendment rights, but that other conclusions are possible.

Applying the theory of equilibrium-adjustment also leads to the conclusion that online contacts should not generate Fourth Amendment rights. Internet

---

128. *Id.* at 277.

129. *Id.*

130. *See* Louise Osborne, *Europeans Outraged over NSA Spying, Threaten Action*, USA TODAY (Oct. 29, 2013, 7:01 AM EDT), http://www.usatoday.com/story/news/world/2013/10/28/report-nsa-spain/3284609.

131. *See* Rebecca Kaplan, *NSA Chief: We Didn't Spy on European Citizens*, CBS NEWS (Oct. 29, 2013, 4:06 PM), http://www.cbsnews.com/news/nsa-chief-we-didnt-spy-on-european-citizens.

technologies destabilize the *Verdugo-Urquidez* inquiry by disrupting the prior relationship between person and place. In *Verdugo-Urquidez*, the police searched the defendant's physical home.[132] A home exists in a single location. It is the place where a person sleeps and keeps his valuables. It is where he pays taxes and participates in a political community. In the context of a physical home, the notion of a connection to a jurisdiction is an all-or-nothing connection. The home implies physical presence, and physical presence brings the full set of connections associated with social and political life.

Internet connections are different. Any person can connect to U.S.-based Internet services from anywhere, and the location of the server is normally hidden from and of little interest to the user. From the user's perspective, services are merely in the cloud. As a result, communicating with a server is divorced from the traditional associations of community and connection to the jurisdiction in which it resides. It is true that some Internet services reflect American values or American success stories. But using such services does not make a foreign national part of the U.S. political community any more than does buying a General Motors car or watching Hollywood movies.

Because Internet services disassociate person and place, recognizing online connections as a basis for Fourth Amendment rights would dramatically alter the preexisting Fourth Amendment balance.[133] Anyone can access U.S. Internet services from anywhere. If online connections can generate rights, then the Fourth Amendment can extend to any person anywhere in the world who uses popular U.S.-based services. Anyone who feared or expected surveillance from the United States could use U.S.-based services strategically in order to obtain Fourth Amendment rights and limit U.S. government surveillance powers. As a practical matter, the U.S. government would be forced to satisfy the hurdles of Fourth Amendment protection all around the world. Recognizing online contacts as a basis for Fourth Amendment rights would effectively replace the territorial Fourth Amendment with a global Fourth Amendment, dramatically altering the global role of the Fourth Amendment because of the fortuity of server location.

To ensure that the role of the Fourth Amendment maintains its preexisting balance as technology changes, the courts should hold that purely virtual contacts with the United States cannot establish Fourth Amendment rights. Fourth Amendment rights should be preserved for those with a physical presence in the United States or a legal association with it. Merely connecting with servers that happen to be located here should not trigger Fourth Amendment protections.

The foregoing analysis may raise the question of whether online contacts should add to the calculus at all. Even if online contacts cannot establish Fourth Amendment rights in themselves, might they add—even only slightly—in a

---

132. *See Verdugo-Urquidez*, 494 U.S. at 262.

133. For a detailed argument about why it is important to maintain the current Fourth Amendment balance in the face of new technologies, see Kerr, *supra* note 22, at 525-29.

case in which a person otherwise falls just short of sufficient contacts? This question is interesting in theory but has little practical importance. At present, the contacts required to establish Fourth Amendment rights under *Verdugo-Urquidez* remain very murky.[134] As a result, identifying a close case is itself difficult. The uncertainty of the *Verdugo-Urquidez* test makes the practical stakes for a possible minor role of online contacts quite small. Given the uncertainty of the *Verdugo-Urquidez* test in general, it seems unnecessary to resolve whether online contacts might add slightly in any particular case.

B. *How Should the Fourth Amendment Apply when the Government Lacks Knowledge of Whether a Monitored Person Has Fourth Amendment Rights?*

The next question asks how the Fourth Amendment should apply when investigators conduct broad monitoring based on a belief, later found out to be erroneous, that a suspect lacked Fourth Amendment rights. To see the problem, imagine investigators are monitoring Internet traffic targeting U.S. government computers. The traffic originates from a proxy server routing anonymized Internet traffic from elsewhere in the world. The use of anonymizing software renders identification of the person and of origins of the traffic difficult or impossible. Assume investigators monitor the traffic freely based on a belief that the target has no rights under *Verdugo-Urquidez.* Later, however, the investigators learn they were wrong. Perhaps the target was a U.S. citizen inside the United States. If the monitoring that occurred would not satisfy Fourth Amendment standards based on the later-discovered facts, how does the Fourth Amendment apply?

There are two plausible answers to this question. On one view, investigators should be fully responsible for their conduct. The officer took intentional action that amounted to a search of a person with Fourth Amendment rights. Under that view, the officer's state of mind is irrelevant, and the Fourth Amendment was violated. On the second view, courts could hold that an officer's reasonable belief that his conduct was lawful either renders it constitutionally reasonable or else eliminates a harsh remedy such as the exclusionary rule. This approach would focus on officer culpability. Because the evidence reasonably supported a belief that the officer's conduct was entirely lawful, the thinking would run, the officer should not be punished for facts that he reasonably could not have known.

In my view, the second approach is better. Courts should hold that a reasonable, good faith belief that monitored individuals lack Fourth Amendment rights under *Verdugo-Urquidez* renders the resulting search constitutionally reasonable. Although a government agent's misunderstanding is regrettable, it is not necessarily culpable. The Fourth Amendment requires reasonableness,

134. *See supra* notes 39-55.

not perfection.[135] A reasonable, good faith belief that the monitored individuals lack Fourth Amendment rights should render the monitoring constitutionally reasonable. The doctrine of apparent authority provides a helpful doctrinal analogy. The apparent authority doctrine arises when the police have a reasonable belief, later shown to be incorrect, that a person has common authority to consent to a search. Under the doctrine, a reasonable but erroneous belief that the third party had authority to consent renders the subsequent search reasonable and therefore constitutional. A similar principle should apply here.

The apparent authority doctrine was introduced in *Illinois v. Rodriguez*, which involved a woman who claimed that she lived in an apartment and invited the police inside to conduct a search there.[136] It turned out that the woman had lied to the police: she had once lived in the apartment but no longer did so.[137] In an opinion by Justice Scalia, the Supreme Court ruled that the officers may have nonetheless acted constitutionally so long as they had a reasonable belief that the woman had common authority over the premises.[138] The reasonableness requirement of the Fourth Amendment requires an officer's conduct to be reasonable rather than correct.[139] So long as the officer had a reasonable belief as to the facts bearing on authority to consent, the Court held, that belief renders the search reasonable:

> The Constitution is no more violated when officers enter without a warrant because they reasonably (though erroneously) believe that the person who has consented to their entry is a resident of the premises, than it is violated when they enter without a warrant because they reasonably (though erroneously) believe they are in pursuit of a violent felon who is about to escape.[140]

The analogy between apparent authority and unknown *Verdugo-Urquidez* status should be clear. In both cases, the police act on a belief at time 1 that they learn at time 2 was false. In both cases, the new facts tell them that their act at time 1 did not satisfy the Fourth Amendment for the factual picture that emerged at time 2.

The reasoning of *Rodriguez* provides a relatively tidy solution to the problem of unknown *Verdugo-Urquidez* status. So long as investigators reasonably believe that their conduct will not obtain protected information from protected individuals at the time it occurs, their resulting Fourth Amendment searches will be constitutionally reasonable. On the flip side, when investigators know or should know that they are obtaining protected information from an individual with Fourth Amendment rights, Fourth Amendment reasonableness requires

---

135. *See, e.g.*, Heien v. North Carolina, 135 S. Ct. 530, 536 (2014) ("To be reasonable is not to be perfect, and so the Fourth Amendment allows for some mistakes on the part of government officials . . . .").

136. *See* 497 U.S. 177, 179-80 (1990).

137. *See id.* at 181.

138. *See id.* at 188-89.

139. *See id.* at 185-86.

140. *Id.* at 186.

satisfying the otherwise-applicable legal standard that presumes *Verdugo-Urquidez* rights.

Implementing this proposal requires addressing two complications. The first is identifying what constitutes a reasonable, good faith belief that a person lacks *Verdugo-Urquidez* rights. For example, if the government is monitoring Internet traffic from an Internet Protocol (IP) address of a computer physically located abroad, does the IP address alone automatically support a reasonable, good faith belief that *Verdugo-Urquidez* rights are absent? Lower court case law interpreting *Rodriguez* suggests that the standard is more demanding than that. According to that case law, the reasonable, good faith inquiry is necessarily fact-specific: bright-line rules do not provide much help.[141] Further, courts do not allow the government to presume apparent authority based on vague and uncertain facts.[142] The government has the burden of proving facts that support a reasonable, good faith belief.[143] If the circumstances are too unclear to support a conclusion, the government cannot rely on those circumstances without making additional inquiries into the facts.[144] Under my proposal, similar limitations would apply to the problem of unknown *Verdugo-Urquidez* status.

Second, my approach implies a time element. When investigators learn new facts and no longer have a reasonable belief that their prior monitoring was lawful, they must adjust to the higher standard. In the case of real-time monitoring, future monitoring must follow the higher standard. But the difference between data collection and data analysis raises an additional complication. In digital evidence cases, agents commonly collect data at one time and then analyze that data later on.[145] That raises the question of how the Fourth Amendment applies if agents collect data when they have a reasonable, good faith belief that the subject of monitoring lacks Fourth Amendment rights, but then they learn, before analyzing the data, that their belief was wrong. The Fourth

---

141. *See, e.g.*, State v. Sawyer, 784 A.2d 1208, 1211 (N.H. 2001) (noting that courts have applied the apparent authority doctrine using a "fact-specific inquiry"); *see also* United States v. Groves, 530 F.3d 506, 509-10 (7th Cir. 2008) (examining factors to be considered in applying the apparent authority test).

142. As the Sixth Circuit has explained,

> [A]pparent authority cannot exist if there is ambiguity as to the asserted authority and the searching officers do not take steps to resolve the ambiguity. "The government cannot establish that its agents reasonably relied upon a third party's apparent authority if agents, faced with an ambiguous situation, nevertheless proceed without making further inquiry. If the agents do not learn enough, if the circumstances make it unclear whether the property about to be searched is subject to mutual use by the person giving consent, then warrantless entry is unlawful without further inquiry."

United States v. Purcell, 526 F.3d 953, 963-64 (6th Cir. 2008) (quoting United States v. Waller, 426 F.3d 838, 846 (6th Cir. 2005)).

143. *See* United States v. Reid, 226 F.3d 1020, 1025 (9th Cir. 2000) (quoting United States v. Shaibu, 920 F.2d 1423, 1426 (9th Cir. 1990)).

144. *Purcell*, 526 F.3d at 963-64 (quoting *Waller*, 426 F.3d at 846).

145. *See, e.g.*, United States v. Hill, 322 F. Supp. 2d 1081, 1087-89 (C.D. Cal. 2004) (describing how computer searches often require an initial seizure of electronic data followed by a subsequent search), *aff'd*, 459 F.3d 966 (9th Cir. 2006).

Amendment might require sealing the previously acquired data pending the issuance of a warrant. Or perhaps it places no limitation at all, on the ground that the initial collection of that evidence was constitutional when it was conducted and therefore can be used even after investigators realize that Fourth Amendment standards should have been followed.

Although the question is difficult, one plausible approach would hinge the answer on the precise timing of when the Fourth Amendment search and seizure occurred. If the government copies data but has not analyzed it, no search has occurred.[146] As I have argued elsewhere, copying without observation generally constitutes a seizure but not a search.[147] On the other hand, if the investigators search the data before copying it into their database by exposing it to observation, the exposure eliminates a constitutional expectation of privacy; subsequent observation does not infringe on Fourth Amendment rights and is not a search.[148] Under this approach, the timing of the search and seizure provides the critical factor. If agents obtain data under a mistaken belief that *Verdugo-Urquidez* left the data unprotected, the initial seizure is reasonable and therefore constitutional. On the other hand, if agents realize that their prior belief was incorrect before searching the data, the Fourth Amendment should apply fully to the subsequent search.

C. *How Should the Law Apply to Monitoring Communications Between Those with and Those Without Fourth Amendment Rights?*

The final question considered in this Part is how the Fourth Amendment should apply to the monitoring of communications between those who have and those who lack Fourth Amendment rights. Imagine investigators are targeting the communications of person *A*, a foreign citizen who lacks Fourth Amendment rights. Person *A* often e-mails person *B*, a U.S. citizen who has Fourth Amendment rights. In ordinary domestic investigative settings, both the sender and the recipient of a communication usually have Fourth Amendment rights in the contents of communications during their transmission.[149] Does *Verdugo-Urquidez* allow the government to monitor the e-mails between persons *A* and *B* without triggering Fourth Amendment oversight, however, be-

146. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551-54 (2005).

147. Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010). For an example of a court adopting this standard expressly, see *In re Search of Info. Associated with [Redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc.*, No. 14-228 (JMF), 2014 WL 1377793, at *3 (D.D.C. Apr. 7, 2014), *vacated on other grounds*, 2014 WL 4094565 (D.D.C. Aug. 8, 2014).

148. *See* Illinois v. Andreas, 463 U.S. 765, 771-72 (1983) ("[O]nce police are lawfully in a position to observe an item firsthand, its owner's privacy interest in that item is lost . . . . Consequently, the subsequent reopening of the container is not a 'search' within the intendment of the Fourth Amendment.").

149. For a detailed overview, see LAFAVE ET AL., *supra* note 126, §§ 4.1-.4.

cause person *A* lacks any Fourth Amendment rights? Or does the surveillance trigger the rights of person *B*, such that the government must limit its monitoring to protect person *B*'s rights?

This question has particular relevance to the constitutionality of monitoring under the controversial provision of the Foreign Intelligence Surveillance Act (FISA) known as section 702.[150] Section 702 authorizes wide-scale Internet monitoring of non-U.S. persons believed to be located outside the United States.[151] In such cases, the non-U.S. person presumably will lack Fourth Amendment rights under *Verdugo-Urquidez*. This raises the question of how the Fourth Amendment applies when the U.S. government monitors the communications of a non-U.S. person outside the United States who happens to be communicating with a U.S. person inside the United States. The U.S. government will end up acquiring the communications of the U.S. person, too. The question is, how does the Fourth Amendment apply when a person with Fourth Amendment rights communicates online with another who does not?

Answering this question requires identifying the proper way to analyze *Verdugo-Urquidez* within Fourth Amendment doctrine. Consider two different approaches. First, we might say that the *Verdugo-Urquidez* inquiry identifies when a Fourth Amendment search or seizure has occurred. When the government breaks into a foreign suspect's home in Mexico, for example, the entry either is not a search or is at least a reasonable search. Alternatively, we might say that *Verdugo-Urquidez* exposes a normally implicit limitation that government action violates the Fourth Amendment only when it implicates a member of "the people" under the Fourth Amendment. Under this view, entry into a foreign suspect's home abroad is still a Fourth Amendment search. The search is lawful, however, because it does not search anyone with Fourth Amendment rights.

This distinction is important because the two approaches arguably point to different doctrinal outcomes. If monitoring a suspect with no Fourth Amendment rights under *Verdugo-Urquidez* does not constitute a search, then the government probably can monitor any communication in which one party lacks those rights without Fourth Amendment oversight. If, however, the *Verdugo-Urquidez* inquiry is an additional inquiry apart from what is a search or seizure, then the government presumably must comply fully with the Fourth Amendment whenever at least one person monitored has Fourth Amendment rights in the data searched or seized. The government conduct is a search or seizure, after all, and the Fourth Amendment requires the government to respect the Fourth Amendment rights held by the U.S. person on one side of the communication.

A brief detour into how the Fourth Amendment applies to communications explains why. The usual Fourth Amendment rule in communications networks is that both sender and receiver have Fourth Amendment rights in the contents

150. 50 U.S.C. § 1881a (2012).

151. *See id.*

of a communication while it is in transit.[152] On the other hand, if two people are on a phone call and one agrees to let the government listen in, the consent of one party allows the government to step in and record the nonconsenting party who is unaware of the government's presence.[153] According to the Supreme Court, the party who does not realize that he is being recorded assumes the risk that the other side is an undercover agent or working with the police.[154] Having shared his communications with the other party, he cannot object to the other party offering up his communications to the police.

Consider the Fourth Circuit's application of this principle in a case involving cordless phone calls, *In re Askin*.[155] A drug dealer named Brumbaugh called his co-conspirator Askin using a primitive cordless phone that communicated using an unencrypted radio signal between the handset and base station.[156] The police listened in by setting up a recording device near the base station of Brumbaugh's phone, and they obtained conversations between the two that implicated Askin.[157] The Fourth Circuit held that the recording of the call did not violate Askin's Fourth Amendment rights because Askin had spoken to an unreliable party. Although Brumbaugh was not a knowing informant, he was an "unreliable recipient[] of the communicated information" because he was using a telephone that broadcast its signal locally.[158] The government was therefore free to monitor all of the calls between Brumbaugh and Askin.

If the *Verdugo-Urquidez* inquiry is understood as an inquiry into what is a search, then it seems plausible to conclude that a person communicating with an individual who has no Fourth Amendment rights waives those rights under *In re Askin*. A person with no Fourth Amendment rights could be deemed unreliable because the Fourth Amendment cannot limit the interception of his calls. By that reasoning, government collection of communications between those with and without *Verdugo-Urquidez* rights cannot be a search, and the Fourth Amendment does not apply.

Although both approaches are plausible, the better conclusion is that the government must satisfy Fourth Amendment standards. Communicating with a person who lacks Fourth Amendment rights should not waive the rights of the person who has those rights. The Fourth Amendment should continue to fully

---

152. *See* United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992) (citing cases); *see also* United States v. Karo, 468 U.S. 705, 726 (1984) (O'Connor, J., concurring in part and concurring in the judgment) ("[T]wo people who speak face to face in a private place or on a private telephone line both may share an expectation that the conversation will remain private . . . ." (citing Katz v. United States, 389 U.S. 347 (1967))).

153. *See* Lopez v. United States, 373 U.S. 427, 439 (1963).

154. *See* Hoffa v. United States, 385 U.S. 293, 303 (1966) (quoting *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting)).

155. 47 F.3d 100, 101 (4th Cir. 1995).

156. *See id.*

157. *See id.* at 101, 103-04.

158. *Id.* at 105.

protect the U.S. person who communicates with those lacking Fourth Amendment rights.[159]

This conclusion rests on three grounds. First, the approach better reflects the reasoning of *Verdugo-Urquidez*. Read closely, *Verdugo-Urquidez* does not purport to address whether the government's conduct constituted a search or seizure. The opening sentence of the majority opinion identifies the issue as "whether the Fourth Amendment applies to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country."[160] The majority's conclusion uses similar phrasing: "Under these circumstances, the Fourth Amendment has no application."[161]

This phrasing presumably was no accident, as it matches the majority's textual reasoning. Because the Fourth Amendment provides "the people" a right against unreasonable searches and seizures, whether an unreasonable search or seizure occurred is distinct from the whether the right applies when the government searches the home of a nonresident alien abroad. The *Verdugo-Urquidez* inquiry acts as an additional limitation on the Fourth Amendment, not as an analysis of whether an unreasonable search or seizure occurred. Indeed, no opinion filed in *Verdugo-Urquidez* questioned whether the government's entry into the home was a Fourth Amendment search; only one Justice addressed whether the search was unreasonable.[162]

Second, even accepting the reasoning of case law such as *In re Askin*, a person who lacks Fourth Amendment rights is not "unreliable" in the same sense as a person who broadcasts his information to the world. A person who lacks Fourth Amendment rights has not taken steps to permit monitoring or increase the risk of being surveilled, such as by consenting to government monitoring or even by using an easily monitored cordless phone. Communicating with a person who lacks Fourth Amendment rights is no different from communicating with servers that lack Fourth Amendment rights, such as in the case of cloud storage. Because the user is not communicating with a party to the

159. Notably, the Justice Department did not challenge this view in a recently filed brief in a case in which the defendant was a U.S. citizen who had communicated with targeted foreign nationals who lacked *Verdugo-Urquidez* rights. *See* Government's Unclassified Response to Defendant's Alternative Motion for Suppression of Evidence & a New Trial at 25-31, United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or. June 24, 2014) [hereinafter Government's Unclassified Response], 2014 WL 4792313.

160. United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

161. *Id.* at 275.

162. Only Justice Stevens addressed whether the government's conduct was an unreasonable search. He concurred on the ground that the Fourth Amendment applied but would have held that the search was reasonable. *See id.* at 279 (Stevens, J., concurring in the judgment). Justice Brennan argued that the Fourth Amendment applied but would have remanded to the court of appeals for review of the record before reaching a conclusion about reasonableness. *See id.* at 294 n.13 (Brennan, J., dissenting) ("Barring a detailed review of the record, I think it is inappropriate to draw any conclusion about the reasonableness of the Government's conduct, particularly when the conclusion reached contradicts the specific findings of the District Court.").

communication that has waived his rights or acted unreliably, communicating with that party should not be deemed a waiver of rights even under the reasoning of *In re Askin*.

Third, the contrary rule offends the principle of equilibrium-adjustment. The Internet has dramatically increased how often we communicate with those abroad. It allows anyone in the United States to communicate with anyone outside the United States instantaneously and without cost. Further, it can be difficult or even impossible for the individual inside the United States to know if his communicant has Fourth Amendment rights. Much communication online is with others who are anonymous or pseudonymous. Treating all communications with those outside the United States who lack Fourth Amendment rights as waivers of Fourth Amendment rights would allow the United States to monitor an increasing percentage of U.S. communications without triggering the Fourth Amendment at all. To maintain the role of the Fourth Amendment in an Internet era, courts should hold that Fourth Amendment rights-holders maintain their rights in communications regardless of the *Verdugo-Urquidez* status of their communicants.

Two caveats should be noted. First, the significance of this rule may hinge on how courts eventually answer the question of when Fourth Amendment rights in communications expire in the course of delivery. In the context of postal mail, a sender's Fourth Amendment rights extinguish when the letter arrives at its destination.[163] For a postal letter, that moment is reasonably clear: postal mail arrives at its destination when the postal service drops it off at the recipient's address. Matters are much less clear with many important kinds of electronic communications. With an e-mail, for example, it is not yet clear whether e-mail arrives at its destination when it arrives at the recipient's server or when the recipient actually accesses a copy. No cases have yet addressed the question.[164] This uncertainty may limit the significance of whether communicating with those who lack Fourth Amendment rights constitutes a waiver. If courts rule that an e-mail arrives at its destination when it reaches the recipient's e-mail server, for example, 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. In that case, the monitoring will occur after the sender's rights have extinguished, and the Fourth Amendment will not limit the monitoring.

A second caveat is that this analysis does not answer the question of when monitoring under section 702 of FISA will satisfy the Fourth Amendment. Un-

163. *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995).

164. Notably, the Justice Department recently argued that the sender's Fourth Amendment rights in an e-mail expire only when the e-mail reaches the actual recipient and not when it reaches the recipient's server. *See* Government's Unclassified Response, *supra* note 167, at 48 n.32. If the government concedes this ground, the concession effectively resolves this uncertainty in litigation against the United States.

der my approach, the government must respect the Fourth Amendment rights of any person with those rights who happens to communicate with a foreign target of monitoring. But what this means will depend on the circumstances. If the government reasonably but mistakenly believes that the individual lacks Fourth Amendment rights, then the monitoring will be constitutional under the good faith analysis in Part II.B. But if the government knows that its monitoring collects the communications of an individual with Fourth Amendment rights, the requirement of reasonableness will depend on the circumstances. Several questions beyond the scope of this Article must be addressed before the constitutionality of section 702 monitoring is resolved.[165]

III. FOURTH AMENDMENT REASONABLENESS AND THE ROLE OF PHYSICAL PLACE

Internet communications regularly travel around the world. Communications can travel almost anywhere in the course of delivery, and they can be collected anywhere they travel.[166] Communications from those abroad routinely travel through or to the United States, and those in the United States routinely send Internet communications abroad.[167] Imagine a person in Paris sends an e-mail using a service provider in California that is destined for another suspect in New York who uses an e-mail service hosted in London. That e-mail could be obtained in California, New York, Paris, London, or any place in between where the communication passes, including at the U.S. border. Once collected by the government, the data can be sent anywhere on the planet for analysis.

This reality of digital communications frames the issue to be considered in this Part: to what extent Fourth Amendment rules should depend on the physical place where the collection occurs. This Article cannot resolve all of the questions raised by evidence collection outside the territory of the United States. In this Part, however, it will address three Internet-specific questions about the intersection between physical location and the Fourth Amendment prompted by the new facts of global computer networks.

The first question is whether the border search exception to the Fourth Amendment applies to electronic communications. Courts have held that the

---

165. *See, e.g.*, United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *15-27 (D. Or. June 24, 2014) (concluding that monitoring under section 702 was reasonable under the Fourth Amendment based on the foreign intelligence exception and general reasonableness balancing).

166. *See* K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J.L. & TECH. 128, 143-46 (2007) (describing the random global route selection process that Internet data utilizes and the ability to collect that data at any switch through which that data travels).

167. The Supreme Court recognized the global nature of Internet communications as early as 1997, describing "cyberspace" as a "unique medium . . . located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet." *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 851 (1997).

border search exception allows broad (and perhaps limitless) searches of physical computers at the international border. An obvious question is whether the same rationale allows surveillance of electronic transmission at the border or its functional equivalent. If an e-mail crosses the border in the course of delivery, does the border search exception allow the government to intercept it?

The second question asks whether the applicable standard of reasonableness depends on where the person is located or where the communication was obtained. Circuit courts have held that extraterritorial searches are governed by a more forgiving reasonableness standard rather than the domestic reasonableness requirement of a search warrant. The global Internet allows communications to be collected in one jurisdiction when the target of monitoring is located in a second jurisdiction. If reasonableness varies by jurisdiction, a choice must be made between the reasonableness standard in the jurisdiction that holds the data and the standard in the jurisdiction that holds the person.

The third question considers whether the standard of reasonableness tracks the jurisdiction of the search or of the seizure when the government seizes data and searches it later in a different jurisdiction. Internet technology enables the government to send collected data to any location for subsequent analysis. In the argot of Fourth Amendment law, the government can seize data in one location but search it in another. If reasonableness varies based on location, and the search and the seizure occur in different locations, should the reasonableness standard be provided by the location of the search or the location of the seizure?

This Part offers the following proposed answers. First, the border search exception should not apply to purely electronic transmission. The border search exception should be read narrowly to avoid eclipsing Fourth Amendment rights online. Construing the border search doctrine as a way to control what enters and exits the United States offers such a limiting principle. Because scanning an electronic transmission does not limit what crosses the border, the border search doctrine should apply to transportation of physical property but not to electronic transmission.

Second, the reasonableness standard should track the location of data rather than people. Adopting a data-focused standard better matches the rationale behind adopting different reasonableness standards in different locations. It also reflects how Fourth Amendment law deals with the separation of property and person in the context of the border search exception. A data-focused standard will also prove easier to implement because the location of data is more readily known and avoids conflicting standards when more than one person has rights in a communication.

Third, if the government collects data in one jurisdiction and analyzes it elsewhere, the reasonableness standard should follow the data collection. Reasonableness should follow the seizure, not the search. This rule is necessary because the government can send data anywhere for analysis; search location is a matter of fortuity or government preference rather than substance. A search-focused rule would give the government undeserved authority in some cases

and impose unjustified restrictions in others. Fourth Amendment protection must rest on more stable and less arbitrary foundations by basing reasonableness on the location of the seizure.

A. *Should the Border Search Exception Apply to Electronic Transmission?*

The first question is whether the border search exception applies to purely electronic transmission. A great deal of world Internet traffic crosses the U.S. border. Some of that traffic crosses the border because it involves one endpoint inside the United States and the other outside it. A person in the United States might access a website located abroad; a person abroad might check his e-mail stored on a U.S. server. In such cases, the Internet traffic must necessarily cross the U.S. border. At the same time, cross-border Internet traffic is more often incidental. Because the Internet is a packet-based global network, Internet communications travel in unpredictable ways. An e-mail sent from New York to Chicago might zip around the world before reaching its destination.[168] The traffic crosses borders because the Internet is designed to carry traffic in ways that are easiest for the network, even though the origin and destination are both within the United States.

This raises a stark choice. If the U.S. government can monitor all Internet traffic entering and exiting the United States from servers located inside the United States, without limit, then the border search exception may be a considerable hole in how the Fourth Amendment protects Internet communications. In the setting of physical mail and packages, courts have held that regional mail-sorting centers where mail and packages enter and exit the country are "functional equivalents of the border" where the border exception applies.[169] The hubs and switches of major Internet access points provide the obvious Internet analogy to those mail-sorting systems. If the border search exception applies, investigators presumably could simply tap into those access points and monitor traffic entering and exiting the United States without Fourth Amendment restriction.

Alternatively, if the border search exception does not apply to electronic transmission, then its absence potentially involves a significant threat to the government's ability to enforce criminal laws through border enforcement. If the government can search physical evidence and machines crossing the border but not purely electronic evidence, then the government may have substantially

---

168. *See* Kim Zetter, *Someone's Been Siphoning Data Through a Huge Security Hole in the Internet*, WIRED (Dec. 5, 2013, 6:30 AM), http://www.wired.com/2013/12/bgp-hijacking-belarus-iceland (describing how e-mail traffic can be sent around the world in the course of delivery).

169. *See* United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008) (en banc) ("The customs search at the Oakland FedEx regional sorting facility took place at the functional equivalent of the border. It should, therefore, be analyzed as a border search." (citation omitted)).

fewer opportunities to search and seize information over the Internet compared to the physical world. As of yet, no court has addressed whether the border search doctrine applies to purely electronic transmission.[170]

There are two primary ways to apply the border search exception to Internet communications. The first is broad and the second is narrow. Under the broad approach, the border search exception should allow the government to search everything entering and exiting the border to know what is entering or exiting the country. So framed, there is no reason to treat digital evidence differently than physical evidence. Because the exception allows inspection of all physical items crossing the border, it should equally allow the inspection of all digital items crossing the border. The fact that so much more of the digital world crosses the border may expand government power, but it has no impact on the legal rule. The exception still applies, regardless of whether the transmission is physical or electronic.

This interpretation is possible, but a narrower approach is also plausible. Under the narrow approach, the border search exception exists to allow the government to keep out items that should be outside the United States and keep in items that should be inside the United States. Although the doctrine is described as a doctrine of searches, it is best understood as a doctrine of seizures: the government has the power to search only to identify items to seize. "[T]he longstanding right of the sovereign" under the border search exception is "to protect itself by stopping and examining persons and property crossing into this country."[171] The underlying right is the right to control what enters and exits the country. Searches are merely a means to that end, required in the physical context only because items need to be searched to be exposed and then blocked from entrance or egress.

The difference between these two approaches is subtle but important. Under the broad approach, the border search exception applies fully to all elec-

---

170. The exception was "the dog that didn't bark" in the Bush Administration's warrantless wiretapping regime disclosed by the *New York Times* in December 2005. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html. The Justice Department issued a white paper defending the lawfulness of the program. *See* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* https://www.epic.org/privacy/terrorism/fisa/doj11906wp.pdf. Somewhat surprisingly, the white paper did not mention the border search exception in defending the constitutionality of the program. Perhaps Justice Department officials concluded that the exception does not extend so far. Alternatively, perhaps the Justice Department did not want to make the argument for other reasons, either because such a conclusion would be politically controversial or because it would require disclosing details as to how the surveillance was conducted.

171. United States v. Ramsey, 431 U.S. 606, 616 (1977); *see also* Carroll v. United States, 267 U.S. 132, 154 (1925) ("Travellers may be so stopped in crossing an international boundary because of national self protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.").

tronic transmissions crossing the border. Under the narrow approach, however, the border search exception should not apply to electronic transmission at all. Surveillance of electronic communications does not and ordinarily cannot block transmission. When the government engages in Internet surveillance, it makes a copy of data and later analyzes that copy.[172] But making a copy does not interfere with transmission: if a person sends a message from point *A* to point *B*, intercepting that communication ordinarily does not block the message from being delivered.

Because the interception of purely electronic transmissions generally involves copying rather than blocking, the narrow approach to the border search exception would not extend to the interception of electronic communications. The result would be a distinction between physical and electronic transmission.[173] Searches of physical devices at the border would trigger the border search exception because evidence once found is then seized. Under the narrow approach, however, electronic searches should not trigger the border search because no subsequent seizure can occur.

In my view, courts should adopt the narrow approach and hold that the exception does not apply to monitoring of purely electronic transmissions solely for the purpose of acquiring information. If a person carries or ships a physical computer or storage disk across the border, the border search exception would apply to a search of the physical device.[174] But if that same person sends the data across the border electronically, without any physical media, the exception should not apply to allow monitoring of the communication to obtain its contents.

Applying the border search exception to electronic transmission is inappropriate because it vastly increases the power of the government. It would allow a happenstance of technology—the particular path that a communication takes—to control the power of the government to monitor communications. Because online communications can easily cross international lines, such a standard would give the government vastly more power to monitor communications of those inside the United States than it has had before. In contrast, rejecting the border search exception for electronic transmission would maintain the status quo of government power. The government would still be able to go outside the United States and collect communications under whatever reasonableness standard applies.[175] But rejecting the exception for purely electronic

172. The NSA's domestic surveillance program provides an example of this process. *See How the NSA's Domestic Spying Program Works*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/nsa-spying/how-it-works (last visited Jan. 28, 2015).

173. *Cf.* Riley v. California, 134 S. Ct. 2473, 2488-91 (2014) (adopting a distinction between physical searches and digital searches in the context of the search incident to arrest exception).

174. How the border search exception would apply to the search of a physical device crossing the border is beyond the scope of this Article. Here, I consider only whether the exception would apply to network transmission.

175. *See supra* Part I.B-C.

transmission prevents matters of technological design from largely eviscerating Fourth Amendment protections online.[176]

Choosing the narrow reading of the border search exception is the flip side of the earlier conclusion that online contacts cannot generate Fourth Amendment rights. In both instances, the fortuity of where online communications travel raises a plausible claim that this fortuity should alter the level of Fourth Amendment protection. To be sure, the two conclusions work in opposite ways. Allowing online contacts to generate Fourth Amendment protection would dramatically expand Fourth Amendment protection; applying the border search exception to electronic transmission would dramatically decrease that protection. But in both cases, the global nature of Internet communications threatens to alter the balance of Fourth Amendment protection. This Article endorses a consistent approach to both problems. In both cases, courts should interpret the ambiguity created by technological change by engaging in equilibrium-adjustment and rejecting interpretations of the Fourth Amendment that would dramatically alter the scope of Fourth Amendment protection.

Although treating physical and electronic searches differently may seem counterintuitive, doing so reflects an important justification for the border search exception: the notion that expectations of privacy at the border are diminished because the border is announced and the prospect of a search is understood. On one hand, that explanation is easy to dismiss because of its circularity. At bottom, it indicates that there is no privacy at the border because people know there is no privacy at the border. But the doctrine also reflects a feature of physical searches that is absent with electronic searches. With a physical search, people generally know when they are crossing the border. Governments mark their international borders with signs and border guards; the border is hard to miss. In the case of electronic transmission, on the other hand, users are often unaware that their communications cross international lines. The global Internet renders borders largely invisible, meaning that users often cannot foresee when their communications will take a path that happens to cross an international line. To the extent the border search doctrine is premised on notice, the lack of notice in the Internet context provides another reason to reject the border search doctrine there.

One complication raised by my approach is that advances in scanning technology can enable monitoring that blocks communications in real time rather than simply collects them for later analysis. For example, Internet service providers often have internal scanning programs designed to detect unwanted communications, such as malware or child pornography.[177] In the future, the

176. This approach echoes the Supreme Court's recent conclusion in *Riley* that the search incident to arrest exception should not extend to cell phones. *See* 134 S. Ct. at 2489-91.

177. For example, AOL maintains a database of the hash values of about 100,000 known images of child pornography and automatically scans e-mails for the hash values. When it finds a match, AOL captures the e-mail, closes the account, and reports the matter to

government might encourage or require providers to install such programs for all international traffic; the software might actually delete the unwanted communication in real time, blocking its transmission, rather than merely copying it during transmission. Such programs would raise the question of whether limiting the border search exception for digital transmission should operate categorically or functionally. That is, the exception might never apply to purely electronic transmissions, or it might not apply to scanning but would continue to apply to monitoring conducted largely or partly with the goal of blocking unwanted communications.[178] Although this Article will not resolve that choice, this potential complication may become increasingly important as scanning technology continues to improve.

B. *Should Fourth Amendment Reasonableness Follow the Person or the Information?*

The next problem is to select the standard for reasonableness for Internet communications obtained abroad. Lower courts have not adopted a consistent approach to reasonableness for extraterritorial searches, leading to disagreement between the Second and Seventh Circuits (on one hand) and the Ninth Circuit (on the other), as discussed in Part I.[179] This discussion will not try to resolve that disagreement, which does not specifically concern the Internet. Instead, it will accept the shared premise that extraterritorial searches trigger some kind of reasonableness analysis. It then considers the resulting cross-jurisdictional problem that arises with global communications networks: What standard of reasonableness should apply when the government collects a communication in a jurisdiction with one standard of reasonableness but the target monitored is in a jurisdiction with a different standard of reasonableness?

Consider a few variations of this problem. First, the U.S. government might intercept a communication outside the United States that was sent by a U.S. citizen located inside the United States. Second, the U.S. government might intercept a communication inside the United States that was sent by a U.S. citizen located outside the United States. Assume that the Fourth Amendment imposes one standard for reasonableness inside the United States and another standard outside the United States. If so, what standard should apply when either the location of the person monitored or the location where the communication is obtained is inside the United States, but not both? Should the

---

the National Center for Missing and Exploited Children. *See* United States v. Ackerman, No. 13-10176-01-EFM, 2014 WL 2968164, at *1-2 (D. Kan. July 1, 2014).

178. The latter approach raises its own difficult questions. Under a functional approach, for example, the standard might be applied communication by communication or program by program. Such a standard also would have to consider programs with mixed purposes, such as a program designed to both acquire communications and block specific subsets of those communications when acquired.

179. *See supra* Part I.B-C.

Fourth Amendment reasonableness standard follow the location of the person or the location of data acquisition?

No cases have focused on this question.[180] Existing precedents generally involve data acquisition in the same jurisdiction as the target. For example, in the Second Circuit's decision on standards for extraterritoriality, *In re Terrorist Bombings of U.S. Embassies in East Africa*, the U.S. government wiretapped the target's Kenyan telephone in Kenya.[181] In the Ninth Circuit's decision in *United States v. Peterson*, the government wiretapped the target's telephone line in the Philippines when he was home.[182] And in the Seventh Circuit's decision in *United States v. Stokes*, the government searched the suspect's home in Thailand when the target was in Thailand.[183] The searches occurred abroad in the same place as the suspects.

Although that trend in the cases is unsurprising, today's Internet renders it increasingly outdated. Internet communications can and do travel around the world.[184] Even a regular telephone call today can be routed anywhere: it is common for today's regular phone calls to travel over Internet lines much like Voice over Internet Protocol (VoIP) calls, meaning that any local call can include packets routed around the world in the course of delivery.[185] Should the standard of Fourth Amendment reasonableness track where the government collects the information or where its owner is located?

In my view, it is preferable for Fourth Amendment standards to follow the location of the information instead of the person.[186] Three reasons support this conclusion: (1) consistency with the rationale of the reasonableness standard,

---

180. In a recently filed brief involving monitoring under FISA's section 702, the Justice Department contended that the standard should be based on where the target of monitoring is located, not where the monitoring occurs. *See* Government's Unclassified Response, *supra* note 167, at 31-32. The district court's ruling in the case did not expressly resolve the question. *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *14-15 (D. Or. June 24, 2014).

181. 552 F.3d 157, 159 (2d Cir. 2008).

182. 812 F.2d 486, 488-89 (9th Cir. 1987).

183. 726 F.3d 880, 886 (7th Cir.), *cert. denied*, 134 S. Ct. 713 (2013).

184. *See* Zetter, *supra* note 176.

185. With the support of major industry players such as AT&T, the old circuit-switching method of telephone communication is being phased out for the more efficient packet-switching model utilized by Internet communications. *See* Jon Brodkin, *AT&T Plan to Shut Off Public Switched Telephone Network Moves Ahead at FCC*, ARS TECHNICA (Jan. 30, 2014, 1:00 AM PST), http://arstechnica.com/tech-policy/2014/01/att-plan-to-shut-off-public-switched-telephone-network-moves-ahead-at-fcc. The Voice Communication Exchange Committee was formed to speed up the transition from the circuit-switching model to the IP model. *See* VOICE COMM. EXCHANGE, http://vcxc.org (last visited Jan. 28, 2015). In short, VoIP is becoming the standard mode of telephone communication.

186. As a result, I would analyze the constitutionality of monitoring under FISA section 702 based on the reasonableness standard inside the United States, not the standard abroad. *Cf. supra* note 188.

(2) consistency with similar rules in other areas of Fourth Amendment law, and (3) a set of practical concerns. I will consider each argument in turn.

First, adopting the reasonableness standard where the information is acquired better matches the primary rationale for replacing the domestic warrant requirement with a generalized reasonableness inquiry for extraterritorial searches. Courts have reasoned that an extraterritorial warrant requirement is superfluous because warrants have no force outside U.S. territory.[187] That claim hinges on the location of property rather than its owners. The effectiveness of the warrant follows the place to be searched, not the person who has Fourth Amendment rights in that place. Because the rationale of the reasonableness standard is keyed to the location of the search, the Fourth Amendment standard should track the location of the search.

This rule may seem intuitive for a physical search. Consider *United States v. Vilar*, a fraud case involving affiliated investment firms with offices in several cities, including New York and London.[188] The U.S. government obtained a U.S. warrant to search the New York office and worked with U.K. law enforcement to obtain a U.K. warrant to search the London office. The U.S. government charged two defendants in New York, and both defendants moved to suppress the fruits of the two searches. Judge Karas first evaluated the lawfulness of the New York search under U.S. law.[189] He then applied the Ninth Circuit's reasonableness standard and evaluated the lawfulness of the London search under U.K. law.[190] The location of the two defendants during these searches was never even mentioned.

Vilar's focus on the location of the search for standards of reasonableness seems intuitively correct. A search is a search. Its reasonableness is naturally gauged by the facts present when the search occurred rather than facts elsewhere. It would seem strange if the Fourth Amendment standard varied depending on the fortuity of whether the defendants happened to be in New York or London at the precise moment the search occurred. And if that intuition seems correct for a physical search, it seems fair to think that the same result should follow in the case of an electronic search. In both cases, reasonableness should follow the location of the search.

Adopting the reasonableness standard that follows where the search or seizure occurs also matches how Fourth Amendment law deals with variances between person location and property location elsewhere. Consider the border search exception. When an individual sends an international letter, the letter crosses the border but the person does not. Courts applying the border search exception focus on the location of the letter rather than the person: the letter can

187. *See In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008).

188. No. S305CR621KMK, 2007 WL 1075041, at *1-2 (S.D.N.Y. Apr. 4, 2007).

189. *See id.* at *18-24.

190. *See id.* at *50-58.

be searched at the border regardless of the location of its sender.[191] Consistency suggests that the reasonableness standard should track the location of the property rather than its owner.

Rooting the reasonableness standard in information location also has significant practical advantages. First, the government is more likely to know the location where it collects information than the location of its owners. The location of a target can be difficult to ascertain. Resting a Fourth Amendment standard on an unknowable fact creates significant uncertainty, making such a standard undesirable.[192] In contrast, the government normally knows the location of a search or seizure that it conducts. If the government obtains the information directly, such as through a direct wiretap, then the government will know where the search occurred based on where the wiretap was installed. If the government obtains information through a third-party provider, the government can consult with the provider to identify where the information originated.[193]

Assessing reasonableness using the location of the information also avoids the puzzle of conflicting standards when multiple individuals have Fourth Amendment rights in a communication. If the reasonableness standard follows the location of the property owner, the government would need to satisfy different reasonableness standards for multiple owners who may be located in different jurisdictions. It is hard to see why the Fourth Amendment should require such a complicated procedure,[194] and this difficulty is avoided by having reasonableness track the location of the interception.

To see the problem, imagine that a U.S. citizen located in foreign country *A* sends an e-mail intercepted in *A* on its way to three U.S. citizens in different foreign countries, *B*, *C*, and *D*. Further assume the Ninth Circuit's reasonableness standard applies: an interception is reasonable if it follows domestic law. In general, both senders and receivers of information retain Fourth Amendment rights in the contents of communications during transmission.[195] As a result, if reasonableness follows the location of the interception, the application of the Fourth Amendment becomes straightforward. The government must satisfy the law in country *A*, the nation where the interception occurs. If reasonableness

---

191. *See* United States v. Seljan, 547 F.3d 993, 999 (9th Cir. 2008) (en banc).

192. *See supra* Part III.

193. Under the legal regimes created by FISA and the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), government agents can obtain communications through third-party providers and are likely in many cases to have preexisting relationships with those providers.

194. *Cf.* New York v. Belton, 453 U.S. 454, 458 (1981) ("[T]he protection of the Fourth and Fourteenth Amendments 'can only be realized if the police are acting under a set of rules which, in most instances, makes it possible to reach a correct determination beforehand as to whether an invasion of privacy is justified in the interest of law enforcement.'" (quoting Wayne R. LaFave, *"Case-by-Case Adjudication" Versus "Standardized Procedures": The* Robinson *Dilemma*, 1974 SUP. CT. REV. 127, 142)).

195. *See generally* LAFAVE ET AL., *supra* note 126, §§ 4.1-.4.

follows the location of the user, however, the government would be required to follow the law in four different countries at the same time, potentially obtaining court orders in all four countries and potentially facing inconsistent standards among them.[196]

The chief counterargument to this position rests on the reality that Internet users may not know in what countries their communications travel or are stored. One rationale for the reasonableness standard is that individuals may expect different privacy rules abroad.[197] If Internet users lack knowledge of where their data is located, a location-based rule may seem to hinge protection on a fortuity. Consider an Internet user in the United States whose communications may end up on a server abroad. Allowing the government to collect information abroad under a lower reasonableness standard instead of a higher warrant standard may erode Fourth Amendment protection based on an accident of how the Internet works and where data is stored.

This is a significant concern, but on balance I find it insufficient to overcome the several arguments in favor of the alternative rule. The concern also rests on the uncertain assumption that reasonableness for extraterritorial searches necessarily implies lower constitutional protection. Perhaps, but perhaps not. For example, under the Ninth Circuit standard of reasonableness that tracks domestic law, the Fourth Amendment standard may be equally protective as or even more protective than the usual Fourth Amendment domestic standard. The scope of privacy protection hinges on the law of the foreign jurisdiction, which may provide as much or more protection than the Fourth Amendment affords domestically.[198] Given the uncertainty surrounding the reasonableness standard for extraterritorial searches generally, the fear that adopting a standard based on the location of the search or seizure will water down standards remains speculative.

---

196. The facts of *Vilar* point to the same problem: If the two defendants in that case were located in different places when the searches occurred, which standard must the government follow?

197. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) (emphasizing "the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad").

198. Notably, the Ninth Circuit extraterritorial reasonableness standard considers the statutory law in the foreign jurisdiction to divine what is reasonable there. *See, e.g.*, United States v. Barona, 56 F.3d 1087, 1095-96 (9th Cir. 1995) (consulting the statutory protections of Danish wiretapping law to identify how the Fourth Amendment applies to wiretapping in Denmark as part of a joint investigation with U.S. authorities). Under the Ninth Circuit standard, it seems, Fourth Amendment protections can be stronger abroad, even if the overall legal standard is similar inside and outside the United States, when the primary protections in both countries are statutory rather than constitutional.

C. *When Data Is Seized First and Searched Later, Should Reasonableness Follow the Search or the Seizure?*

A final wrinkle to consider is what rules should apply if the government collects data in one jurisdiction and then analyzes it in another jurisdiction. For example, the government might collect data abroad and then send the data to the United States for analysis. Or the opposite might occur: the government might collect data domestically and send it outside the United States for analysis. Once again, we encounter the prospect of a seizure first and a search second.[199] Three different rules might conceivably apply. First, the Fourth Amendment might track the legal standard where the data was searched; second, it might track the legal standard where the data was seized; and third, the law might bifurcate the questions so that the search and seizure are each analyzed in the jurisdiction where they occur.

We can quickly reject the first option of applying the law where the data is searched. When the government seizes first and searches later, its agents control where the search will occur. Data can be sent anywhere on the Internet at the press of a button, and the location where the government analyzes the data is essentially arbitrary. If the law followed the jurisdiction where the search occurred, the government could collect information anywhere and send it to the jurisdiction with the lowest privacy protection for analysis. It makes little sense to select a rule designed to limit government power that would allow the government to so easily game the rules to expand its power. Indeed, such a race to the bottom would conflict with the requirements of equilibrium-adjustment. It would expand government power for reasons of technological fortuity—namely, the ability to readily send electronic information to any jurisdiction.

Similar concerns render the second option of tracking where the data was seized preferable to the third option of evaluating the search and seizure differently based on the rules where each occurred. The location where the search occurs remains arbitrary and subject to the government's control. If the government seizes data inside the United States, it is hard to see why piping the data outside the United States should enable a greater power to search through the information abroad. And the flip side remains true as well. If the government collects data outside the United States, it is hard to see why stronger privacy protections should apply simply because the government may bring the data inside the United States for analysis. When the government seizes first and searches second, the location of the search is a question of government convenience and should not alter the government's authority.

The en banc Ninth Circuit reached an analogous conclusion in *United States v. Cotterman*, the case involving a border search of a laptop computer.[200] Agents seized Cotterman's laptop at the U.S.-Mexico border but then shipped it

199. *See* United States v. Hill, 459 F.3d 966, 973-75 (9th Cir. 2006).

200. 709 F.3d 952, 956 (9th Cir. 2013) (en banc).

170 miles to a computer forensic expert in Tucson, Arizona, for analysis.[201] Cotterman argued that the usual border search exception could not apply because the search had occurred in Tucson. In his view, the distance from Tucson to the border rendered the search an "extended border search" requiring reasonable suspicion.[202] The Ninth Circuit disagreed on the grounds that the agents had seized the laptop at the border and the location of the search had no impact on Cotterman's privacy rights.[203] According to the court, a different Fourth Amendment rule is not triggered "simply because the device is transported and examined beyond the border."[204]

Although *Cotterman* arises in a different context than that considered here, its focus on the location of the seizure rather than the subsequent search should apply equally in the Internet setting. The underlying principle applies throughout this Article, as it aims to translate from territorial facts to global facts: location-based rules that are fortuitous or easily gamed should not provide the basis for Fourth Amendment protection. Just as courts should not allow targets of monitoring to gain protection under *Verdugo-Urquidez* based on the fortuity of where the servers they use reside,[205] and courts should not allow the government to gain powers to seize or search digital transmission at the border based on the fortuity of where Internet traffic passes,[206] neither should courts allow Fourth Amendment protection to rise or fall depending on the fortuity of where the government sends data for analysis. Fourth Amendment protection must rest on more stable principles, such as physical or legal relationships with the United States and the location where the government collects the data it will then analyze.

CONCLUSION

This Article has attempted to solve a series of difficult and novel Fourth Amendment problems raised by the global Internet. Putting the proposed answers together creates the following structure. First, Fourth Amendment rights should be reserved for those with offline contacts with the United States; online contacts should not suffice. Second, if the government reasonably believes that a person lacks Fourth Amendment rights, monitoring of that person is lawful as long as that belief remains objectively reasonable. On the other hand, as soon as the government no longer reasonably believes that a person lacks Fourth Amendment rights, the government must fully respect that person's Fourth

201. *See id.* at 958.

202. *Id.* at 961.

203. *See id.* at 962 ("Because Cotterman never regained possession of his laptop, the fact that the forensic examination occurred away from the border, in Tucson, did not heighten the interference with his privacy.").

204. *Id.* at 961.

205. *See supra* Part II.A.

206. *See supra* Part III.B.

Amendment rights even if he is communicating with others who lack (or are believed to lack) Fourth Amendment rights.

The standard of reasonableness that applies under the Fourth Amendment should be based on the location where the data was collected rather than the location of the person with rights in that data. Further, the government should not be able to rely on the border search exception to justify a lower standard (or no standard) of reasonableness to acquire electronic transmissions for the purpose of collection. The reasonableness standard that applies should be the full standard based on the location of the data whenever a person has established Fourth Amendment rights. If the government collects data inside the United States for a U.S. person abroad, the usual warrant standard should apply. If the government collects foreign-stored or foreign-acquired data for a U.S. person in the United States, the extraterritorial reasonableness standard should govern its acquisition.

These proposed rules do not answer every question raised by the extraterritorial application of the Fourth Amendment to the Internet. However, they offer a coherent framework for applying the Fourth Amendment in a way that maintains the existing territorial conception of the Fourth Amendment to a global computer network. The global Internet threatens to dramatically destabilize Fourth Amendment law by disassociating person, place, and data. The proposed rules aim to protect the Fourth Amendment by blocking its evisceration while at the same time maintaining its fundamental balance. They ensure the role of the Fourth Amendment as we translate it not only from a physical world to a networked environment but also from a local investigative environment to a global one.