ESSAY

ELECTRONIC SURVEILLANCE AT THE VIRTUAL BORDER

Susan Freiwald[*]

Before the advent of globalization, physical borders between countries played the crucial role in differentiating legal systems. Travelers from one country to another usually knew that they were also moving out of one system of laws into another. In most cases, they either encountered physical landmarks, or they had to get past border officials who controlled passage. A nation-state made its own laws that it imposed on the people within its border, including, of course, those who had crossed into its territory. Borders separated those subject to both the burdens and privileges of a nation's laws from those subject to neither. In short, borders distinguished the area in which a particular sovereignty was exercised from the areas in which it was not.

As Professors Johnson and Post observed in an influential essay in the Stanford Law Review, cyberspace has fundamentally challenged the efficacy of traditional physical borders.[1] Internet users can easily "visit" web sites established in a foreign country without that country's government being

[*] Professor, University of San Francisco School of Law. I thank Peter Volz for his excellent research assistance and Gretchen Harris and the other editors of the Mississippi Law Journal. I also thank Patricia L. Bellia, Leah Freiwald, Gus Guibert, and Peter Jan Honigsberg for their helpful comments. Any errors are mine.

[1] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

aware of their "arrival." The dramatic increase in electronic movements across borders, whether as communications or transactions, has meant that the traditional physical means of policing borders no longer work as effectively.[2] Johnson and Post argued that the "borderlessness" of cyberspace calls into question both the efficacy and legitimacy of "territorial sovereign" regulation of cyberspace.[3] They argued that cyberspace citizens should play a greater role than traditional sovereigns in setting the legal rules to govern cyberspace.[4] Their proposal garnered substantial academic response, with some vocal critics proclaiming that traditional legal rules based on territorial sovereignty still functioned well, notwithstanding the move into the electronic sphere.[5]

Johnson and Post published their essay on cyberspace borders in 1996, in the early days of the World Wide Web. Since then, lawmakers have drafted numerous laws designed specifically to address new problems arising in cyberspace.[6] Here in the United States, for example, Congress has designed new rules to handle intellectual property infringement based in cyberspace,[7] and has tried several times to regulate indecency online, only to have its statutes overturned by the Supreme Court's application of the First Amendment to cyberspace.[8]

---

[2] *Id.* at 1372; *see also* LAWRENCE LESSIG, CODE VERSION: 2.0, 10-11 (2006) (discussing borderlessness of cyberspace and its implications).

[3] Johnson & Post, *supra* note 1, at 1370-76.

[4] *See id.* at 1374.

[5] *See, e.g.*, Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); *see also* Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 485-89 (2000) (arguing that self-governance is inconsistent with liberal ideas).

[6] *See generally*, *e.g.*, PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE (3d ed. 2007).

[7] Digital Millennium Copyright Act ("DMCA"), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.); *see also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435 (2d Cir. 1991) (describing the DMCA as something "Congress enacted in 1998 to strengthen copyright protection in the digital age").

[8] *See, e.g.*, Ashcroft v. ACLU, 542 U.S. 656, 674 (2004) (rejecting a statutory attempt to "regulate the vast content of the World Wide Web at its source" as too costly to "First Amendment values"); Reno v. ACLU, 521 U.S. 844, 870 (1997) (noting that "our cases provide no basis for qualifying the level of First Amendment scrutiny that should be

Meanwhile, courts have interpreted pre-cyber statutes in new cyberspace contexts and have extended common law precedents into cyberspace settings.[9] It therefore seems right to assume, at this point, the legitimacy of a sovereign's imposition of its own legal rules on the cybercitizens within its physical territory.[10]

I. THE VIRTUAL BORDER FOR ELECTRONIC SURVEILLANCE PURPOSES

Instead of considering the physical regulation of virtual activities, in this essay I consider how a virtual border regulates physical activities. In particular, I consider how the law has created intangible borders to regulate government surveillance of communications. These intangible borders function the same way as physical borders functioned historically. They demarcate those "places" in which our government imposes burdens and grants privileges from those "foreign places" in which it does neither.[11] In this essay, I focus on the requirements imposed by the Fourth Amendment, under which government agents interested in monitoring communications must comply with a set of demanding procedures. As I will discuss, when the Fourth Amendment applies, it requires extensive judicial oversight of government surveillance investigations, before, during and after the surveillance takes place.[12]

The Fourth Amendment does not protect everyone, however. It mandates the greatest judicial oversight when

applied to" the Internet).

[9] *See, e.g.*, Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123-24 (W.D. Pa. 1997) (proposing a new sliding scale test for determining jurisdiction in cyberspace); Intel Corp. v. Hamidi, 71 P.3d 296, 302-12 (Cal. 2003) (resolving how the trespass to chattels doctrine applies to bulk e-mails sent by a disgruntled employee to his former employer).

[10] However, the exercise of sovereignty over foreigners whose online actions affect local residents remains the subject of considerable debate. *See, e.g.*, Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisémitisme, 433 F.3d 1199 (9th Cir. 2006) (en banc) (dismissing on jurisdictional grounds a case that considered whether French parties' could enforce a domestic judgment against an American company whose web services in France were found to violate French law).

[11] In this context, I mean that our laws do not directly regulate the conduct of foreign persons in foreign countries, not that our practices impose no burdens on them.

[12] *See infra* Part II.A.

government agents monitor, for law enforcement purposes, the communications of "U.S. Persons"[13] in America.[14] At the opposite end of the spectrum, the Fourth Amendment has nothing to say about government surveillance of the communications of foreign persons in foreign places to gather foreign intelligence.[15] When they want to monitor entirely "foreign" communications, executive branch agents enjoy considerable discretion. That is in part because such surveillance falls within the executive's constitutional power to conduct foreign affairs,[16] and in part because foreigners surveilled abroad generally lack standing to bring cases in United States courts.[17] As the Fourth Circuit has noted, "[j]ust as the separation of powers . . . forced the executive to recognize a judicial role when the President conducts domestic security surveillance, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance."[18]

The executive's decision whether to monitor foreigners abroad derives from its foreign policy prerogatives, which the President exercises subject to limited involvement by the other two branches.[19] While the Senate approves of diplomats and

[13] Under Fourth Amendment doctrine, U.S. citizens and aliens with "sufficient connection with this country to be considered part of th[is] community" have the same rights. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). Federal statutory law refers to American citizens and permanent resident aliens as "U.S. Person[s]." 50 U.S.C. §§ 1801(i), 1821(1) (2005). Throughout this essay, the term "U.S. Persons" will be used to represent the group of citizens and aliens who have Fourth Amendment rights.

[14] *See infra* Part II.A.2.

[15] *See infra* Part II.B.1.

[16] *See, e.g.*, United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 319 (1936) (discussing the President's foreign affairs powers); *see also* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case*, 41 U.C. DAVIS L. REV. 1259 (2008) (describing and critiquing the foreign affairs argument for the President to have the power to conduct warrantless electronic surveillance for foreign intelligence).

[17] *See infra* Part II.B.1.

[18] United States v. Hung, 629 F.2d 908, 914 (4th Cir. 1980) (citation omitted).

[19] *See Curtiss-Wright*, 299 U.S. at 318. As I will discuss, when government agents cannot monitor foreigners without at the same time monitoring U.S. Persons, then the Fourth Amendment comes into play. *See infra* Part III.

consents to treaties and Congress controls military funding, the President alone decides whether to recognize foreign governments and what type of foreign relations to establish.[20] The executive branch's portfolio includes the monitoring of foreigners' communications abroad. Part of the foreign affairs function includes deciding whether to gather such intelligence in the first place and what to do with it if it is obtained.[21]

That a member of the judiciary must be intimately involved in purely domestic surveillance for violations of domestic crimes and that the executive branch has discretion over purely foreign surveillance of foreign people in foreign places seems clear.[22] But many, if not most, surveillance operations are neither purely domestic nor purely foreign, which substantially complicates the analysis. In fact, regulation of government surveillance of communications depends on so many factors that the rules Congress has formulated to handle them seem almost impenetrably complex.[23]

The pertinent statutory provisions may be found in the Foreign Intelligence Surveillance Act ("FISA").[24] Those rules currently grant more discretion to executive branch monitors when (1) the purpose of the investigation is to gather foreign intelligence information rather than information pertaining to criminal offenses, (2) the target of the surveillance is located in a

[20] That is not to say that the scope of the President's foreign affairs prerogatives may not be contested by both courts and Congress.

[21] I do not wish to minimize the enormity of the questions posed by surveillance of mixed domestic and foreign targets, but rather to suggest that some investigations are in fact purely across the virtual border. For further discussion of the problem of foreign surveillance investigations that target foreigners but end up listening in on Americans, see *infra* Part III.

[22] *See, e.g.*, *Hung*, 629 F.2d at 908 (describing the different considerations attendant to foreign intelligence surveillance and domestic criminal investigations).

[23] *See, e.g.*, Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 628-29 (2007) (describing "the fabled complexity of the [modern electronic surveillance statute] and the difficulty of applying it to new technologies" (footnote omitted)); Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283 (2005) (describing how modern electronic surveillance law handles spyware and identifying several points of complexity and uncertainty).

[24] *See* Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

foreign country rather than in the United States, (3) the monitoring itself is conducted in a foreign place rather than in the United States, (4) the target is a foreign citizen rather than a U.S. citizen or a resident alien, (5) the U.S. Person targeted communicates with someone in a foreign country rather than here, (6) there is probable cause to believe that the U.S. Person targeted is an agent of a foreign power rather than there being no association between the target and a foreign power.[25] Any one scenario involves some combination of the above pairings, which makes it even more difficult to determine the correct rule.

While the FISA scheme is a creature of Congress, it must conform to constitutional constraints.[26] As Part II discusses, Fourth Amendment precedents require the judiciary to oversee executive branch surveillance of purely "domestic" surveillance.[27] But the Fourth Amendment has much less, if anything, to say about executive branch conduct of purely "foreign" surveillance.[28] One could defensibly arrange the scenarios along a spectrum from most "domestic," and therefore protected by the Fourth Amendment, to most "foreign," and therefore least protected.

Rather than viewing the Fourth Amendment as providing decreasing judicial oversight as the character of the electronic surveillance becomes increasingly foreign, however, one could instead view Fourth Amendment protection as being all or nothing. In other words, one could view the Fourth Amendment as providing strict regulation for purely domestic investigations

---

[25] *See generally* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS, § 11:2 (2007) (detailing the applicable statutory provisions).

[26] Note that the most recent amendments to FISA have been challenged in court for violating the First and Fourth Amendments and separation of powers. *See* Complaint at 3, 42, Amnesty Int'l USA v. McConnell, No. 08 CV 06259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf. On the other hand, the Bush administration has challenged FISA itself as an unconstitutional intrusion on the President's inherent authority as commander-in-chief. *See* ACLU v. NSA, 438 F. Supp. 2d 754, 780 (E.D. Mich. 2006) (rejecting government's claim that the executive branch had "inherent power" to conduct warrantless surveillance of international communications).

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

[28] *See infra* Part II.B.

and no regulation for purely foreign investigations because the latter are governed by executive branch discretion. Then one would view the rules for cases that fall in the middle as designed to determine whether to treat the investigation as domestic or foreign. Under this view, in cases that are neither clearly domestic nor clearly foreign, the judge's role would be to review the executive's decision to deprive the target of judicial oversight of the surveillance that the Fourth Amendment mandates. The executive makes such a determination when a target effectively acts in the interest of a foreign power; in such a case, the executive may be said to "exile" that target if she is a U.S. Person.[29]

In this analysis, the virtual border plays a key role. On this side of the virtual border, domestic targets enjoy extensive judicial review of executive branch surveillance, pursuant to the dictates of the Fourth Amendment.[30] On the other side, foreign targets are subject to whatever electronic surveillance the executive branch chooses to conduct in the exercise of its foreign affair powers.[31] Foreign targets have no right to complain about surveillance techniques in our courts, though they may of course raise their complaints in their own courts.[32]

That is not to say that judicial review over mixed domestic and foreign cases is not mandated by the Fourth Amendment, but rather that judicial oversight in these cases plays an additional role besides keeping electronic surveillance within permissible bounds. In addition, judges review the executive

[29] *See infra* Part II.C (describing the FISA rules that regulate "exiling").

[30] *See infra* Part II.A, III.

[31] This is the case until the executive effectively brings them back over the border by prosecuting them, at which time the investigation becomes more like a domestic law enforcement investigation. *See, e.g.*, United States v. Hung, 629 F.2d 908, 914 (4th Cir. 1980) (discussing how the Fourth Amendment rights of the target change at the point that the investigation becomes "primarily" about law enforcement instead of foreign intelligence gathering). *But see* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006) (noting concern that past attempts to distinguish between foreign intelligence and law enforcement investigations, based in part on the *Hung* case, inhibited cooperation between executive branch agents).

[32] *See, e.g.*, Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 153 (D.D.C. 1976) (holding that an Austrian citizen subject to electronic surveillance by U.S. Army personnel in Berlin had no standing to sue in U.S. courts).

branch's decision to exile and ensure that U.S. Persons are not deprived of their Fourth Amendment rights either by being exiled over the virtual border without sufficient cause, or by being swept up in the surveillance of exiled U.S. Persons and foreigners.[33] The Fourth Amendment also calls for admitting foreign people inside our virtual border in some cases. For example, resident aliens and those with sufficient connections to this country who are targeted in ordinary criminal investigations benefit from the highest level of Fourth Amendment protection of their communications, even though they are not American citizens.[34]

By viewing the Fourth Amendment regulation of electronic surveillance as "on" for surveillance of people on the domestic side of the virtual border and "off" for those on the foreign side of the border, one can get a clearer view of how much is at stake in the "exiling decision." With that in mind, one can appreciate the importance of judicial oversight of the executive's decision to exile and can assess the rules governing that decision by how well they protect against improper exile.[35] Again, while one may view judicial review in these cases as quasi-constitutional Fourth Amendment protection,[36] one should also evaluate the judiciary's performance of its responsibility to oversee the exiling decision.

As mentioned, FISA contains the rules that determine the

[33] The surveillance of U.S. Persons who had not been "exiled" during the course of targeting those on the other side of the virtual border has caused considerable controversy in recent years in the wake of revelations about extensive surveillance by the NSA pursuant to a program called the "Terrorist Surveillance Program" ("TSP"). *See infra* note 146; *see also infra* Part III (discussing that controversy and Congress' response).

[34] *See infra* Part II.C.2 (discussing the "naturalization" process).

[35] For example, one could criticize the rules pertaining to electronic surveillance of the Internet as providing insufficient judicial oversight of the executive's decision to deprive cyber-citizens of Fourth Amendment rights. Under my formulation, the executive would be effectively exiling cybercitizens without a sufficient demonstration of "foreign" conduct. A full discussion of that problem is beyond the scope of this essay.

[36] *See, e.g.*, Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 458-59 (2005) (describing the FISA procedures as "quasi-constitutional" but casting doubt on the constitutionality of recent amendments).

amount of review provided by a judge over the exiling decision.[37] As will be discussed in Part II, those rules permit the executive branch to use special procedures that accord meaningfully fewer rights to foreign targets.[38] Foreign targets include those who are neither American citizens nor resident aliens (which together constitute "U.S. Persons"). But such targets also include those U.S. Persons who have effectively become foreigners through virtual exile. To exile a U.S. Person across the virtual border, high level executive branch officials must have probable cause to believe that the U.S. Person targeted for exile works as an "[a]gent of a foreign power,"[39] and the officials must seek "foreign intelligence information"[40] about that agent. If a reviewing judge approves the executive branch's showing, agents may conduct surveillance of the exiled target without according her the full Fourth Amendment rights granted to domestic targets.[41]

Importantly, and unlike in the domestic context, the "exiled" target does not have to receive notification of the surveillance unless and until the executive decides to bring criminal charges against the target based on the evidence gathered.[42] The lack of notice enhances the executive's discretion to conduct surveillance of exiled people, because it reduces the likelihood that the executive's decision to exile and its surveillance thereafter will face a challenge in court.[43] As I mentioned earlier and will further discuss, on this side of the virtual border, where full Fourth Amendment rights apply, judges must actively keep executive branch surveillance within prescribed bounds throughout all phases of the investigation and must provide notice to the target when the surveillance

[37] *See* Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[38] *See infra* Part II.B.

[39] 50 U.S.C. § 1801(b) (Westlaw through July 2008 amendments).

[40] § 1804(a)(7)(B) (2000).

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

[42] *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1039 (D. Or. 2007).

[43] *See infra* text accompanying notes 145-156 (discussing the difficulty of bringing cases challenging FISA surveillance).

concludes.[44]

The FISA rules require a judge to review the executive's decision to exile a U.S. Person across the virtual border.[45] Because a U.S. Person loses a significant constitutional right—the right to substantial judicial oversight of executive branch surveillance—when she is exiled across the virtual border, the banishment decision must not be made lightly. The executive branch cannot be trusted to make those decisions unfettered because it would have an incentive to treat all U.S. Persons as foreigners, merely to avoid Fourth Amendment constraints.[46] History amply demonstrates that executive branch agents find it tempting to move as many people across the virtual border as possible in order to avoid penetrating judicial oversight.[47]

A special court, the Foreign Intelligence Surveillance Court ("FISC") oversees the executive branch's attempts to exile U.S. Persons over the virtual border.[48] The FISC operates in private, ex parte, and generally without publishing its decisions in order to protect the secrecy of the executive branch's counterintelligence and counterterrorism operations.[49] When the FISC reviews the executive branch's claims that a U.S. Person has been acting sufficiently "foreign" to justify exile, it operates as an essential check on executive discretion.[50]

In this essay, I develop the concept of the virtual border and

---

[44] *See infra* Part II.A.1.

[45] *See infra* Part II.C.1 (discussing specifics of the FISA rules).

[46] Although FISA procedures do accord some protections that are similar to those provided to domestic targets, such as the minimization requirement, it is not clear that those protections are constitutionally mandated. *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002). In addition, my point is not that the FISA procedures for judicial review do not accord rights, but that their function is meaningfully different from the function served by judicial review of executive branch surveillance in the domestic context.

[47] *See generally* KRIS & WILSON, *supra* note 25, Chap. 3 (recounting how history of executive branch abuses of surveillance powers spurred congressional regulation); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004); *see also infra* Part III (discussing implications of tendency for executive branch to abuse surveillance powers).

[48] *See* 50 U.S.C. § 1803 (Westlaw through July 2008 amendments).

[49] Bellia, *supra* note 36, at 460-74 (arguing for greater transparency surrounding the proceedings of the FISC).

[50] See *infra* Part II.C.1 for a full discussion of the FISA procedures.

illustrate how the FISA rules are designed to ensure U.S. Persons are not improperly deprived of their Fourth Amendment rights by exile. The goal is to provide a new way to evaluate the foreign surveillance laws based on whether they provide adequate judicial review of the executive's decision to exile. In recent years, for example, the foreign surveillance rules have been both amended and flouted in ways that weaken this essential function.

Because this paper aims to promote an understanding of how the electronic surveillance laws are supposed to function, it focuses first and most thoroughly on how they are designed to work under applicable constitutional precedents rather than how they have been significantly altered by recent amendments or ignored altogether.[51]

Part IIA of this essay discusses the Fourth Amendment precedents that establish who is on this side of the virtual border and the extensive judicial review accorded to government surveillance of those people. Then, Part IIB reviews the Fourth Amendment precedents that establish who is on the other side of the virtual border, whether they are physically located outside of this country or not.[52]

In Part IIC, I describe how FISA requires that government agents interested in conducting electronic surveillance of U.S. Persons have to convince a judge that they are seeking foreign intelligence information about targets who are agents of a foreign power before they may deprive those targets of their Fourth Amendment rights. As a result, U.S. Persons in this country enjoy either the protections of full judicial review of executive branch surveillance, or judicial oversight of the determination to exile them over the virtual border where they

[51] A more extensive analysis of the ways in which the current executive branch abuses reflect insufficient judicial oversight of the exiling decision is planned for a subsequent paper.

[52] Because this essay considers the border between domestic criminal cases and foreign cases, it does not inquire into state surveillance laws. For a thorough and important discussion of wiretapping at the state level, see Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L. J. 971 (2003).

no longer benefit from those protections.[53]

Part III of this essay considers recent changes and challenges to judicial review of the exiling decision. In the past several years, the FISA rules have expanded executive branch discretion in ways that dramatically weaken judicial oversight of the exiling decision.[54] At the same time, officials in the Bush administration appear to have extensively abused their electronic surveillance tools in the wake of the tragic attacks on September 11, 2001, by exiling U.S. Persons with insufficient justification.[55] Finally, recent practices of all three branches have made it difficult for challenges to the exiling process to be heard in court. [56]

The reality of executive branch overreaching reinforces the need for extensive judicial review of electronic surveillance on this side of the virtual border as well as effective judicial review of executive branch decisions to exile people across the virtual border. But while executive branch abuse of electronic surveillance has been egregious during the Bush administration,[57] it threatens to persist afterwards if members of the judiciary play an unduly circumscribed role in overseeing executive actions.

---

[53] Here I am using the formulation under which one has all Fourth Amendment rights in the domestic context and none over the virtual border.

[54] *See infra* Part III.

[55] *See, e.g.*, JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2008) (detailing extensive NSA surveillance of Americans without obtaining the requisite judicial review); Hepting v. AT & T Corp., 439 F. Supp. 2d 974, 992-94 (N.D. Cal. 2006) (considering class action claim against large telecommunications company for aiding the NSA in conducting illegal surveillance); Curtis Bradley et. al., *On NSA Spying: A Letter to Congress*, 53 N.Y. REV. OF BOOKS 2 (2006), *available at* http://www.nybooks.com/articles/18650.

[56] *See, e.g.,* FISA Amendments Act of 2008, Pub. L. No. 110-261,122 Stat. 2436 (providing for courts to dismiss pending and future actions challenging any assistance provided to the "President's Surveillance Program" or "Terrorist Surveillance Program" if the Attorney General certifies that the assistance was authorized by the President to detect, prevent, or prepare for a terrorist attack).

[57] *See, e.g.*, JAMES X. DEMPSEY & DAVID COLE, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY (2d ed. 2002); KRIS & WILSON, *supra* note 25; Swire, *supra* note 47, at 1325-29.

II. ESTABLISHING THE VIRTUAL BORDER

A. On this Side of the Virtual Border

1. Rigorous Judicial Review of Electronic Surveillance Investigations

When the government uses electronic surveillance to monitor communications, it significantly intrudes on privacy.[58] While a consensus on what "privacy" is remains elusive, there is no doubt that when the government listens in on its citizens' communications, it violates their privacy by inhibiting their right to be let alone and by raising the risk that they will face negative consequences for their speech.[59] Supreme Court Justices have historically taken a jaundiced view of government surveillance of communications, with some regarding it as a "dirty business,"[60] and others recognizing that there is perhaps no greater threat to freedom than that posed by government surveillance of our communications.[61] As Justice Powell wrote in 1972, "[t]here is, understandably, a deep-seated uneasiness and apprehension that th[e] [electronic surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens."[62]

Electronic surveillance does, however, provide government agents with a powerful investigative tool.[63] More than fifty

---

[58] *See generally* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 95 (2000) (describing both the privacy intrusions inherent in electronic surveillance by government and the history of legal regulation of such surveillance).

[59] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972); *see also* Maclin, *supra* note 16, at 1285-87.

[60] Olmstead v. United States, 277 U.S. 438, 470 (1928) (Holmes, J., dissenting).

[61] *See, e.g.*, Berger v. New York, 388 U.S. 41, 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."); Lopez v. United States, 373 U.S. 427, 470 (1963) (Brennan, J., dissenting) ("If electronic surveillance by government becomes sufficiently widespread, and there is little prospect for checking it, the hazard that as a people we may become hagridden and furtive is not fantasy.").

[62] *Keith*, 407 U.S. at 312.

[63] *See, e.g.*, *id.* at 311-12 ("The covertness and complexity of potential unlawful

years ago, advocates for electronic surveillance argued that the dramatic rise in organized crime and the difficulty of infiltrating its networks with informants or undercover agents mandated law enforcement use of electronic surveillance.[64] By 1968, a sufficient consensus had emerged for Congress to pass the Wiretap Act,[65] according to which government agents could use electronic surveillance to investigate crimes, subject to a set of stringent procedural requirements. Those limitations came directly from two Supreme Court cases decided the prior year.

In the landmark cases of *Katz v. United States*[66] and *Berger v. New York*,[67] the Supreme Court recognized the strength of the law enforcement rationale for permitting some investigative use of electronic surveillance by the government.[68] At the same time, the Supreme Court emphasized in both cases the considerable risk to privacy posed by electronic surveillance of our communications.[69] For that reason, the Court refused to let the executive branch determine for itself whether sufficient cause justified its use of electronic surveillance and the Court refused to "retroactively validate" the government's conduct, because agents had proceeded without "prior judicial sanction."[70] Thus, the *Katz* Court found the executive branch's interception

conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances.").

[64] *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 15-42 (2004) (reviewing the history of the passage of the Wiretap Act).

[65] Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351, 82 Stat. 212, (codified as amended in scattered sections of 18 U.S.C. §§) (1968) ("Wiretap Act"). Prior to the passage of the Wiretap Act, twenty-one members of the Senate supported a bill to permit electronic surveillance by government agents to protect national security, but not for ordinary crime control. *See* S. REP. NO. 90-1097, at 161 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2223.

[66] 389 U.S. 347 (1967).

[67] 388 U.S. 41 (1967).

[68] *See id.* at 63.

[69] *See id.* at 56; *Katz*, 389 U.S. at 353.

[70] *Katz*, 389 U.S. at 356; *see also id.* at 356-57 ("[The Supreme] Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.").

of the contents of the target's telephone call to violate the Fourth Amendment because the government had neither obtained a prior warrant nor established an exception to the warrant requirement.[71] The Court emphasized that "subject only to a few specifically established and well-delineated exceptions," none of which would likely apply to electronic surveillance, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment."[72]

In *Berger*, the Supreme Court provided more guidance about what the Fourth Amendment requires when it struck down a New York statute that authorized law enforcement use of electronic surveillance.[73] The Court identified some of the features of electronic surveillance that necessitated close judicial review of its use. The Court noted that because electronic surveillance, as compared to a traditional search of a house, is hidden, continuous, intrusive, and indiscriminate, it poses a heightened threat to the target's privacy.[74] The Court opined that absent "adequate judicial supervision" executive branch use of electronic surveillance devolved into the general warrant that the Framers clearly proscribed as a violation of the Fourth Amendment.[75] To properly reduce the risks and intrusion inherent in electronic surveillance, the Court enunciated several procedural requirements with which executive branch officials must comply before they may engage in electronic surveillance.[76]

The *Berger* Court's requirements, which Congress codified in the 1968 Wiretap Act,[77] are all designed to ensure that

---

[71] *Id.* at 358.

[72] *Id.* at 357.

[73] *See Berger*, 388 U.S. at 57-60.

[74] *See id.* at 59-60; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 10-11. *See also id.* at ¶¶ 50-56 (discussing how courts made the same findings regarding video surveillance and applied the core features of the Wiretap Act to that practice as a matter of Fourth Amendment law).

[75] *Berger*, 388 U.S. at 60.

[76] *Id.* at 63.

[77] Note that there is some dispute about just which of the requirements in the Wiretap Act are constitutionally required. *See, e.g.*, United States v. Koyomejian, 970 F.2d 536, 542-51 (9th Cir. 1992) (en banc) (Kozinski, J., concurring).

surveillance is used only in those cases in which executive branch agents may demonstrate a strong need to a court, prior to initiating the surveillance. In the Act, Congress requires a tight nexus between the target of the search and probable cause to believe that the target is engaged in a serious crime, as well as specificity regarding which conversations investigators seek.[78] In addition, agents have to establish that less intrusive methods of investigation are not possible.[79] Courts also oversee the surveillance while it takes place by requiring that agents report periodically on their progress and minimize the interception of non-incriminating conversations.[80] After the electronic surveillance ends, courts review submitted transcripts to determine whom, besides the target, should receive notice.[81] Courts hear claims by those surveilled that agents acted illegally and grant the exclusion of evidence, as well as damages, when those claims are successful.[82] In sum, the Fourth Amendment, as codified in the Wiretap Act, requires executive branch agents to submit to rigorous judicial oversight before, during and after their use of electronic surveillance to investigate.

2. Clear Residents: U.S. Persons Suspected of Domestic Crimes

The cases that established the requirements of rigorous judicial oversight, *Berger* and *Katz*, involved law enforcement investigations of U.S. citizens suspected of domestic crimes. In other words, the targets in those cases did not even arguably fall within the foreign affairs concerns of the executive branch.[83] Subsequent cases and statutory provisions have addressed what to do in cases that implicate both foreign affairs and Fourth Amendment rights, but all have taken for granted that

[78] *See* Freiwald, *supra* note 64, at 23-26 (reviewing the Wiretap Act requirements).

[79] 18 U.S.C. § 2518(3)(c) (2006).

[80] § 2518(5).

[81] § 2518(8)(d).

[82] § 2515.

[83] *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308 (1972) (describing the *Berger* and *Katz* cases as involving "the surveillance of crimes unrelated to the national security interest").

electronic surveillance within this country by domestic law enforcement of citizens may proceed only by meeting the heightened requirements set out in *Berger* and *Katz* and codified in the Wiretap Act.

3. U.S. Persons Threatening Domestic Security Are Also Residents

An important question that neither *Berger* nor *Katz* resolved was what power the President retained to conduct surveillance without meeting the requirements set out in those two cases.[84] Apparently, presidents had been authorizing warrantless electronic surveillance based on the need to protect the national security for decades prior to passage of the Wiretap Act, and they continued to do so after 1968.[85] The Wiretap Act did not address that executive practice, but instead specifically declined to "limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."[86]

In *Keith*, the Supreme Court considered a challenge by a domestic group which the Attorney General viewed as a "national security" threat to the executive branch's warrantless surveillance of its communications.[87] The executive branch supported its practices on the ground that it needed more leeway to investigate threats to national security because such threats required specialized and secretive intelligence techniques that varied meaningfully from those used in

---

[84] *See* Katz v. United States, 389 U.S. 347, 358 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

[85] *See Keith*, 407 U.S. at 299 ("Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees . . . ."(footnote omitted)); *see also id.* at 310 n.10; Bellia, *supra* note 36, at 430-31 (reviewing history).

[86] 18 U.S.C. § 2511(3) (1972) (amended 1978).

[87] *Keith*, 407 U.S. at 300-01; *see generally* Maclin, *supra* note 16, at 1279-320 (discussing the background to the *Keith* case and its modern applicability).

investigations of ordinary crimes.[88] According to the Attorney General, the surveillance of the defendants had been "'necessary to protect the nation from attempts . . . to attack and subvert the existing structure of Government.'"[89]

Before turning to the merits of the constitutional claim, the Supreme Court rejected the government's claim that the Wiretap Act's language specifically authorized the executive to conduct warrantless surveillance to protect national security.[90] The Court found that in the Wiretap Act, Congress had "simply left presidential powers where it found them."[91]

Having dispensed with the statutory argument, the Supreme Court recognized the perennial conflict between the executive branch's desire to conduct surveillance without submitting to rigorous judicial review, and the constitutional requirement that the judiciary retain an active role in keeping such surveillance within defensible limits to protect citizens' rights. The Court formulated its task as "examin[ing] and balanc[ing] the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."[92]

Ultimately, the Court determined that, while the executive's compelling interest in protecting the country against domestic threats does exceed its interest in enforcing the criminal laws, subjecting national security surveillance to a Fourth Amendment warrant requirement would not "unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it."[93] Moreover, the Court decided that because "Fourth Amendment freedoms [could not] properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive

---

[88] *Keith*, 407 U.S. at 318-19.

[89] *Id.* at 309 (quoting the Attorney General's affidavit).

[90] *Id.* at 303.

[91] *Id.* Congress eventually removed the provision in the Wiretap Act that the government had relied on to claim Congressional approval of its actions in *Keith*.

[92] *Id.* at 314-15.

[93] *Id.* at 315; *see also id.* at 320-21.

Branch," investigators and prosecutors could "not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[94] Under the Court's reasoning, even their participation in activities that threaten the very existence of their country is insufficient justification to exile Americans across the virtual border where they would be deprived of rigorous judicial oversight of law enforcement surveillance.

Interestingly, the Supreme Court emphasized that both Fourth Amendment and First Amendment values supported subjecting executive branch surveillance practices to rigorous judicial oversight. The Court recognized that the executive branch would necessarily cast a suspicious eye on those who espoused views contrary to its programs and policies, and would be inclined to view such actors as posing a threat to "domestic security."[95] But if such suspicions were sufficient to justify the use of so intrusive a technique as electronic surveillance, that would pose a serious threat to citizens' ability to exercise their First Amendment rights of assembly and speech. Speakers might refrain from criticizing the executive branch for fear of surveillance and retaliation, in direct contradiction of core constitutional values. As the Court dramatically expressed it:

> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[96]

The *Keith* Court affirmed the need for "[p]rior review by a neutral and detached magistrate" of the executive's decision to use electronic surveillance.[97] The Court required executive

---

[94] *Id.* at 316-17.

[95] *See id.* at 314 ("History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies.").

[96] *Id.* at 314.

[97] *Id.* at 318. The Court ruled that reliance on "post-surveillance judicial review" alone would be insufficient. *Id.* The Court clearly contemplated judicial review both before and after the surveillance took place. *Id.* at 321.

branch agents to submit to the requirements of prior judicial review whenever they sought to investigate U.S. Persons for violation of our laws, unless those U.S. Persons were suspected of having a "significant connection with a foreign power, its agents or agencies."[98]

The Court recognized that different procedures could apply in cases involving domestic security rather than ordinary crime because of differences in purposes and methods.[99] In particular, the Court suggested that the greater need for secrecy in investigations might require that surveillance applications be made to a member of a specially designated court; that the difficulty in identifying the exact targets might require a different standard than the probable cause standard in the Wiretap Act; and that the more long-range and preventative nature of the investigation could support longer time periods and less stringent reporting requirements.[100] However, the Court refused to excuse the executive branch from obtaining prior judicial approval when it used electronic surveillance to investigate U.S. Persons.[101]

Congress might have responded to the *Keith* decision by drafting a special set of procedures for surveillance of U.S. Persons suspected of domestic terrorism, or domestic threats to national security. Had it done so, the procedures could have been a watered-down, or at least adjusted, set of Fourth Amendment requirements pursuant to the *Keith* Court's recognition that procedures less rigorous than those under the Wiretap Act could regulate such cases.[102] But Congress did not do that.[103]

Instead, Congress accepted the Court's invitation to draft special rules, but designed them to apply only in situations

---

[98] *See id.* at 309, n.8 (defining "domestic organizations" as having no such connections).

[99] *Id.* at 322-23.

[100] *Id.*

[101] *Id.*

[102] *See id.*; Banks & Bowman, *supra* note 58, at 52-53.

[103] *See generally* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 803 (1989) (describing the passage and provisions in FISA).

involving foreign powers and their agents. The procedures codified in FISA provide for the FISC to hear claims brought by the executive branch that the target of its surveillance efforts is either a foreign power or an agent of a foreign power, and that the executive seeks "foreign intelligence information" about that target.[104] So while Congress presumably could have provided a different, and somewhat more lenient, set of procedures for those cases when the government investigated Americans viewed as threats to national security, instead it required that American targets become more foreign before they may be targeted using the FISA procedures.[105]

To summarize, participation in activities viewed by the executive branch as threats to national security is insufficient to exile a U.S. Person over the virtual border to the place where the executive branch has more discretion to conduct surveillance pursuant to its power over foreign affairs. Instead of drawing a line solely based on the nature of the threat, FISA draws the line based on the "foreignness" of the target investigated. At some point a U.S. Person's foreign conduct is enough to exile that person over the virtual border into a "foreign land" of executive discretion rather than judicial oversight of their surveillance.

4. U.S. Citizens Abroad

U.S. citizens enjoy some Fourth Amendment protection of their communications even when they are outside the physical confines of the United States.[106] This further illustrates the

---

[104] 50 U.S.C. § 1801(e) (2006).

[105] *See* Banks & Bowman, *supra* note 58, at 95 (noting anomaly that U.S. Persons targeted in domestic terrorism investigations are subject to the same procedures as such persons targeted for violation of U.S. crimes, despite the fact that the domestic terror threat may be just as great as the foreign terror threat).

[106] Reid v. Covert, 354 U.S. 1, 5 (1957) ("[W]e reject the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights."); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 160 (D.D.C. 1976) (noting requirement that federal officials "present for approval in the United States a warrant for a wiretap [of an American citizen] overseas"). In a decision issued just as this essay was going to press, the Second Circuit recognized the Fourth Amendment rights of U.S. citizens surveilled abroad by U.S. agents, but interpreted those rights to require reasonableness

virtual, rather than physical, nature of the border that separates the area in which targets are subject to the protections of the Fourth Amendment from the foreign space in which they are not. In one case, *Berlin Democratic Club v. Rumsfeld*, the court considered the Fourth Amendment rights of "a number of American citizens and organizations and one Austrian citizen" living in Berlin who claimed they were subject to an extensive campaign of illegal electronic surveillance and harassment by the U.S. Army.[107] Based on the *Keith* decision, the court found that the Fourth Amendment compelled government investigations to obtain judicial authorization prior to conducting electronic surveillance of the Americans living in Berlin.[108] It is important to note that the court found that even though the American citizens and their organizations were overseas, there was "no evidence of collaboration with or action on behalf of a foreign power."[109] Thus, when U.S. agents monitor "domestic" U.S. citizens abroad, they do so subject to the protections of the Fourth Amendment.[110] By leaving U.S. territory, American citizens do not automatically leave the protections of the Fourth Amendment behind.

B. On the Other Side of the Virtual Border

1. Foreigners Abroad

Because the Supreme Court necessarily stays out of cases that fall clearly within the foreign affairs power of the President

rather than a warrant. See United States v. Odeh (*In re* Terrorist Bombings of U.S. Embassies in East Africa (Fourth Amendment Challenges)), 548 F.3d 276, (2d Cir. 2008).

[107] *See Berlin Democratic Club*, 410 F. Supp. at 147-48.

[108] *See id.* at 156-57.

[109] *See id.* at 159.

[110] See *id.* at 156-57. Note that the Justices have not entirely agreed about just what the Constitution requires when applied abroad. *See, e.g.*, *Reid*, 354 U.S. at 74 (Harlan, J., concurring) (disagreeing with the notion that "every provision of the Constitution must always be deemed automatically applicable to American citizens in every part of the world"); *but see id.* at 8-9 (majority opinion) ("While it has been suggested that only those constitutional rights which are 'fundamental' protect Americans abroad, we can find no warrant, in logic or otherwise, for picking and choosing among the remarkable collection of [constitutional] 'Thou shalt nots' . . . ." (footnote omitted)).

and because of jurisdictional issues, few cases squarely address the Constitutional rights of foreign people in foreign places. In the *Berlin Democratic Club* case described above, the court found that the Austrian citizen, who was apparently subject to the same electronic surveillance as the Americans, could not bring a claim. The Austrian citizen lacked standing to sue because, as a "citizen of a foreign country," he was "not subjected to the laws of this country" and he could "utilize the laws of his own country to protect himself."[111]

Foreign citizens may not generally complain in U.S. courts when our government conducts surveillance of them outside this country. Congress has some power over the executive branch's foreign surveillance through its power of the purse,[112] and the executive may face both domestic and foreign challenges to whatever surveillance practices become known.[113] But when the surveillance monitors purely foreign citizens in foreign countries, it is beyond the power of the U.S. courts to address. What makes government surveillance in foreign places of foreign people constitutionally controversial is the substantial risk that U.S. Persons will be caught up in the monitoring, which is a problem discussed in Part III.

2. Foreigners Here but Without Sufficient Connection

The story is different when the foreigner bases his claims to Fourth Amendment protections on some connection to the United States, which could be either the foreigner's presence here when surveilled or his prosecution here. These cases help illustrate the virtual border between those targets subject to rigorous judicial review under the Fourth Amendment and those

---

[111] *Berlin Democratic Club*, 410 F. Supp. at 153. The court noted that it would have been different if the United States had tried to prosecute the Austrian citizen in the United States or if he had applied for relief under a U.S. statute that permits relief to a non-resident alien. *See id.* at 152.

[112] *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 15 (1972) (noting that Congress, but not the courts, should monitor the "wisdom and soundness of Executive action").

[113] *See generally* BAMFORD, *supra* note 55 (reporting on NSA surveillance after the September 11 attacks); JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY (2001) (chronicling NSA surveillance efforts before September 11, 2001).

not so protected.

In the case of *United States v. Verdugo-Urquidez*,[114] the defendant sought to have evidence obtained during a search of his home in Mexico, conducted by U.S. agents in concert with Mexican officials, excluded from his trial in the United States on drug-trafficking charges. The Supreme Court found that the defendant's mere presence in the United States for trial was insufficient to entitle him to rights under the Fourth Amendment.[115] The Court distinguished precedents in which aliens had been granted constitutional rights as involving aliens who had "come within the territory of the United States and developed substantial connections with this country."[116] The Court based its decision in part on a reading of "the people" in the text of the Fourth Amendment.[117] The Court also expressed concern that recognizing Fourth Amendment rights in aliens abroad "could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."[118]

A subsequent case applied the reasoning in *Verdugo-Urquidez* to a case involving a Russian citizen suspected of computer hacking.[119] A federal district court held that the defendant, Gorshkov, could raise no Fourth Amendment complaint about a remote search of his computer in Russia, even though he had visited undercover officers in the United States as part of a sting operation.[120] The court found that "a single entry into the United States that is made for a criminal purpose is hardly the sort of voluntary association with this country that

---

[114] 494 U.S. 259 (1990).

[115] *Id.* at 271 (rejecting defendant's claim to Fourth Amendment protection on the ground that he was "an alien who has had no previous significant voluntary connection with the United States").

[116] *Id.*

[117] *Id.* at 265 ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." (quoting U.S. CONST. amend. IV)).

[118] *Id.* at 273-74.

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

[120] *Id.* at *3.

should qualify Defendant as part of our national community for purposes of the Fourth Amendment."[121]

A person may come to qualify for Fourth Amendment protections only by actions which ground him sufficiently on this side of the virtual border, actions that neither Verdugo-Urquidez nor Gorshkov accomplished. These cases thus illustrate the difficulty for foreigners of getting over the virtual border into this country. Being here physically is not enough. The next section considers what is enough to move one onto the domestic side of the virtual border and what is enough to justify banishment.

C. Crossing the Virtual Border

1. Statutory Procedures for Border Movements

a. Of U.S. Persons

Under FISA, executive branch officials may not banish U.S. Persons across the virtual border without first convincing a judge of probable cause to believe the target is an agent of a foreign power and that other requirements have been met.[122] Before they may conduct surveillance of U.S. Persons, executive branch officials must submit a detailed application with affidavits from investigators, a certification from a high-ranking official and the Attorney General's approval.[123] The application must establish probable cause to believe that the target is an "agent of a foreign power" when the target is a U.S. Person.[124] That roughly means the target has engaged in spying for a

---

[121] *Id.*

[122] *See, e.g.*, KRIS & WILSON, *supra* note 25 (describing FISA procedures); Bellia, *supra* note 36, at 436-48 (same).

[123] *See* Kris, *supra* note 31, at 490 (citing 50 U.S.C. § 1804).

[124] 50 U.S.C. § 1804(a)(3)(A) (Westlaw through July 2008 amendments). The government must also show that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2)(B) (Westlaw through July 2008 amendments).

foreign power, sabotage or international terrorism.[125] After amendments made by the USA PATRIOT ACT ("Patriot Act"),[126] a U.S. Person may not be considered to be an agent of a foreign power based solely on speech or actions protected by the First Amendment.[127] Presumably that requirement reflects the Supreme Court's concern in *Keith* that the executive branch might make a claim of national security necessity to conduct surveillance actually designed to silence or harass unpopular views.[128]

The FISA procedures themselves require the FISC to review the executive's showing, but to accord it considerable deference. The FISC reviews both the claim that the target is an agent of a foreign power, and the executive branch's assertion that the proposed surveillance is designed to gather "foreign intelligence information."[129] The whole system operates on the premise that the executive requests permission to conduct surveillance free of the Wiretap Act requirements only when there is sufficient evidence to justify it, which is why FISC denial of executive branch requests is so rare.[130]

For those investigations in which the executive branch succeeds in having the FISA procedures apply rather than the Wiretap Act, the regulations differ considerably.[131] As

[125] § 1801(b); Kris, *supra* note 31, at 491-92.

[126] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272.

[127] *See* 50 U.S.C. § 1805(a)(2)(A) (2000 & Supp. 2001); 50 U.S.C. § 1842(a)(1) (2000 & Supp. 2001); KRIS & WILSON, *supra* note 25, at § 8:37; Bellia, *supra* note 36, at 447;

[128] *See supra* Part II.A.3. It is not altogether clear how this protection would be enforced, particularly in light of plaintiffs' standing problems in FISA cases. *See, e.g.*, *In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1131-35 (N.D. Cal. 2008) (illustrating the difficulty of establishing oneself as an "aggrieved person" under FISA when one cannot use evidence protected by states' secrets).

[129] § 1804(a)(6)(B).

[130] *See* Bellia, *supra* note 36, at 459 (reporting that between 1979 and 2006, only twenty-one of 17,000 FISC orders were challenged, and none of the challenges were successful). Of course it is possible that the judges on the FISC are loathe to second guess the executive's decision to exile because they view it as properly within the President's discretion. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) (discussing executive's discretion in the field of foreign affairs).

[131] *See* Banks & Bowman, *supra* note 58; Bellia, *supra* note 36, at 439-42.

previously discussed, agents who succeed in meeting the FISA requirements may conduct surveillance for longer periods, and they may refrain from giving notice to the target unless and until the target faces prosecution on criminal charges.[132]

FISA thus endeavors to ensure that the executive branch decision to exile a U.S. Person is not made lightly and is subject to review. The procedures, including review by a secret court and the accompanying limited public disclosure, balance the executive's need to have discretion over its foreign affairs power with the judiciary's duty to ensure that the Fourth Amendment has real meaning.

b. Of Foreign Persons

As discussed above, when foreign citizens have sufficient connection to the United States to fall under the umbrella of U.S. Persons, they are entitled to the Fourth Amendment protections of judicial review and are treated the same as a U.S. citizen. But those who lack that connection are not. FISA establishes detailed procedures for targets of surveillance who are not U.S. Persons, meaning they are neither citizens nor permanent residents, and those procedures accord significantly less protection.

Thus, the executive branch may conduct surveillance of non-U.S. Persons, under FISA, on a showing that they are linked to a foreign power.[133] It is easier to establish that the agent is seeking foreign intelligence information with regard to non-U.S. Persons, and the application is reviewed only for completeness rather than clear error.[134] In addition, unlike U.S. Persons suspected of foreign intelligence activities, foreigners in this country may be surveilled without any concern that First Amendment protected activities have provided the only basis for the surveillance.

---

[132] *Compare* Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding procedures dramatically different), *with In re* Sealed Case, 310 F.3d at 737-42 (finding procedures comparable).

[133] *See* 50 U.S.C. § 1801(b)(1) (Westlaw through July 2008 amendments); Kris, *supra* note 31, at 490-92.

[134] 50 U.S.C. § 1805(a)(4) (Westlaw through July 2008 amendments).

2. When the Fourth Amendment Requires Naturalization

Some non-resident aliens, even those monitored abroad, may acquire the right to bring Fourth Amendment challenges to their surveillance. In one scenario, those monitored abroad but then brought to the United States for prosecution have been found to have standing to bring Fourth Amendment challenges to their surveillance.[135] It is also possible that an alien abroad could somehow fit within the *Verdugo-Urquidez* test of having sufficient connection to the United States to raise a Fourth Amendment claim to U.S. government surveillance abroad.[136] Either way, the fact that foreign people subject to government surveillance abroad may, in some cases, bring a Fourth Amendment challenge to that surveillance reinforces the notion that the line dividing Fourth Amendment protected targets from those who are not is much more virtual than physical.

III. RECENT CHANGES AND CHALLENGES TO JUDICIAL REVIEW AT THE VIRTUAL BORDER

Although the *Keith* Court recognized that the Fourth Amendment protections accorded to U.S. Persons who acted in concert with foreigners could differ dramatically from those targeted for domestic crimes and national security, it neither

[135] *See, e.g.*, United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974) (foreign citizen wiretapped abroad entitled to bring Fourth Amendment claim when the government sought to introduce evidence obtained thereby in a criminal case against him in the United States); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 152 (D.D.C. 1976) (stating as an exception to the general rule that non-resident aliens have no standing in United States courts: "when a non-resident alien is brought from abroad to appear for and be the subject of a domestic criminal prosecution"); *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 279 (1990) (Brennan, J., dissenting) (arguing that when government agents enforce U.S. criminal laws abroad, they do so subject to the Fourth Amendment).

[136] *See, e.g.*, Douglas I. Koff, *Post*-Verdugo-Urquidez*: The Sufficient Connection Test – Substantially Ambiguous, Substantially Unworkable*, 25 COLUM. HUM. RTS. L. REV. 435 (1994) (arguing in favor of an expansive approach to finding non-resident aliens searched abroad by U.S. government agents subject to the protections of the Fourth Amendment). *But see* Randall K. Miller, *The Limits of U.S. International Law Enforcement After Verdugo-Urquitez: Resurrecting Rochin*, 58 U. PITT. L. REV. 867, 885 (1997) (arguing that aliens outside the United States should have no protection under the Fourth Amendment).

defined what actions counted nor did it specify what protections, if any, would be accorded. As the Court wrote in *Keith*,

> No doubt there are cases where it will be difficult to distinguish between 'domestic' and 'foreign' unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case.[137]

Perhaps surprisingly, the question of exactly how the Fourth Amendment regulates foreign intelligence surveillance of U.S. Persons remains unanswered by the Supreme Court. Though some decisions issued in the period after *Keith* and before passage of FISA assumed that the President's power over foreign affairs included the right to conduct warrantless surveillance for foreign intelligence purposes, others questioned that proposition.[138] In a recent case issued by the Foreign Intelligence Surveillance Court of Review ("FISCR"), which met for the first time to consider whether the FISC had properly found amendments made by the Patriot Act to violate the Fourth Amendment, the FISCR opined that the constitutional question about how the Fourth Amendment regulates foreign intelligence surveillance remained unresolved both before and after it issued its decision.[139]

The FISCR's decision addressed whether FISA's procedures adequately ensured that agents did not follow FISA standards in cases more properly pursued as law enforcement investigations regulated by the Wiretap Act.[140] The FISCR concluded that the statute satisfied the Fourth Amendment, even though the new provisions permit agents to follow FISA procedures whenever a

---

[137] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 309 n.8 (1972).

[138] *Compare In r*e Sealed Case, 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002) (recognizing precedents holding that the President had inherent executive authority to conduct warrantless foreign surveillance searches), *with* Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975) (en banc) (plurality opinion) (finding warrantless surveillance for foreign intelligence purposes to be constitutionally unreasonable). *See also* Bellia, *supra* note 36, at 435-36 (reviewing this history).

[139] *See In re* Sealed Case, 310 F.3d at 746.

[140] *See id.* at 737-46.

significant purpose of the investigation is to gather foreign intelligence information. Before the Patriot Act amendments, agents had to show that the primary purpose, instead of a significant purpose, was to gather foreign intelligence information.[141]

The FISCR's decision has generated significant criticism in academia, and a federal district court has specifically rejected it.[142] In *Mayfield v. United States,* the district court in Oregon held FISA, as amended, to be facially invalid under the Fourth Amendment because the provisions too easily permitted the executive branch to deprive a U.S. Person of full Fourth Amendment rights without a sufficient showing of probable cause.[143] Whether or not the *Mayfield* court's analysis stands up to review, the court addressed the conditions under which executive branch agents may exile U.S. Persons and expressed concern about the adequacy of the executive's showing.[144]

Both the FISCR and *Mayfield* opinions considered whether FISA's procedures provided adequate judicial oversight of the executive's showing to justify exile. Both illustrated that the decision to exile a person has significant implications for that person's rights, and that the exiling process itself must meet constitutional standards. However, both cases may rarely, if ever, be replicated, because of the difficulties involved in challenging exiling decisions.[145]

---

[141] *Id.* at 746. *See generally* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007) (assessing the impact of the Patriot Act amendments); Kris, *supra* note 31 (describing the impact of the new language on executive branch procedures).

[142] Mayfield v. United States, 504 F. Supp. 2d 1023, 1041-42 (D. Or. 2007).

[143] *Id.* at 1037.

[144] The *Mayfield* court's concern that a U.S. Person can be surveilled under FISA without probable cause to believe the target is guilty of a crime conflicts with how others read the pertinent provisons. One expert describes FISA as requiring a showing of suspected criminality before U.S. Persons may be targeted. *See, e.g.*, Kris, *supra* note 31, at 491 ("U.S. Persons can be agents of a foreign power only if they engage in some level of criminal activity.").

[145] The FISCR case was the first decided by that court. The FISCR reviewed the FISC's determination that the executive's procedures violated the Constitution. *In re* Sealed Case, 310 F.3d 717, 717 (Foreign Int. Surv. Ct. Rev. 2002) . In *Mayfield*, the target of allegedly unlawful surveillance brought a facial Fourth Amendment challenge to the government's surveillance of him, which the court granted despite the

In practice, the Fourth Amendment may constrain the executive branch's exiling decisions in ways that are not enforced and for which the victims receive no remedy. For example, to the extent that no one who is willing or able to challenge it learns of executive branch surveillance that violates the Fourth Amendment, that transgression will go unremedied. When Congress or the courts deny a court's power to review past transgressions, those transgressions escape punishment.

It seems clear that, in recent years, the executive branch has violated the Fourth Amendment rights of U.S. Persons by improperly exiling them — or depriving them of their full Fourth Amendment rights of judicial review. There has been reporting of extensive surveillance of the communications of U.S. Persons not suspected of being foreign agents as part of an extensive Terrorist Surveillance Program ("TSP") instituted in the wake of the September 11th attacks.[146] Plaintiffs, and their expert witnesses, have charged that the communications of U.S. Persons with foreign ties, if any, that are insufficient under the Fourth Amendment to justify exile, were nonetheless swept up in an extensive surveillance effort conducted by the National Security Agency.[147] Because that program proceeded without prior judicial review, as required by the Wiretap Act and FISA, such surveillance appears to have violated the Fourth Amendment.[148]

Acts by both Congress and the courts have made it less likely that the victims' Fourth Amendment rights will be vindicated. First, the Sixth Circuit denied standing to a group of plaintiffs and held that they could not establish that they had

governments' efforts to claim that he lacked standing. *Mayfield*, 504 F. Supp. 2d at 1023. *See also supra note* 128 (describing hurdles to bringing challenges to FISA).

[146] *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008); Bamford, *supra* note 55; Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287 (2008); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[147] *See* Complaint, Hepting v. AT & T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. 06-CV-00672).

[148] *See* Maclin, *supra* note 16, at 1293-326 (arguing that the *Keith* case establishes the unconstitutionality of the TSP).

been injured by the TSP because state secrets prevented them from amassing evidence about the program.[149] Under the state secrets privilege, the executive may keep some foreign affairs information out of court and away from the public, to protect its need for secrecy.[150] Secondly, in recent amendments to FISA, Congress agreed to dismiss pending and future cases that challenged the assistance provided by telecommunications companies to the NSA as part of the TSP.[151] As a result, the NSA's conduct as well as that of the intermediaries may never face judicial review, and any Fourth Amendment violations will go unpunished and unremedied. Finally, those same amendments also reduced the amount of oversight that the FISC will give to exiling decisions by permitting the executive branch to submit protocols for surveillance rather than individualized cases for consideration.[152] Critics fear that the amendments provide insufficient oversight of the executive branch and effectively authorize "dragnet surveillance" that will sweep up the communications of innocent people without justification.[153] Civil liberties groups have challenged the amendments' constitutionality.[154]

---

[149] ACLU v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007). The Sixth Circuit recognized state's secrets as a bar to plaintiffs' efforts to acquire information about their surveillance by the NSA and therefore denied plaintiffs standing to sue. *Id.* That decision reversed ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (finding challenged NSA surveillance to violate the First, Fourth, and Fifth Amendments and other constitutional and statutory provisions).

[150] *See, e.g.*, *Hepting*, 439 F. Supp. 2d 974 (discussing state secrets privilege). *But see In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109 (N.D. Cal. 2008) (holding that the FISA provisions for judicial access to foreign surveillance information preempt the states secrets privilege, which is a creature of federal common law).

[151] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 110-261, §30, 122 Stat. 2436, 2468 (amended 2008).

[152] *See id.* at 2437-67.

[153] *See, e.g.*, Press Release, ACLU, Senate Passes Unconstitutional Spying Bill and Grants Sweeping Immunity to Phone Companies (July 9, 2008), *available at* http://www.aclu.org/safefree/general/35928prs20080709.html.

[154] *See, e.g.*, Complaint, Amnesty Int'l USA v. McConnell, No. 08 cv 06259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf; Motion to Dismiss, *In re* Nat'l Sec. Agency Telecomms. Records Litig., No. 06-1791 VRW (N.D. Cal. Oct. 17, 2008), *available at* http://www.eff.org/files/filenode/att/immunityoppocorrected.pdf (challenging constitutionality of grant of immunity to telecommunications company in the FISA

That executive branch agents may deprive people of their constitutional rights and face no repercussions is clearly a problem. Yet the controversy generated by these cases will likely yield some important reforms. For example, the FISA Amendments provide for review of the TSP and a report to Congress.[155] Litigation over the telecommunications company's involvement in the TSP has already generated important precedents about the appropriate use of the state secrets privilege.[156] All of these cases, and particularly the scandals, focus the public on the need for meaningful and sufficient judicial review of the executive branch's exiling decisions and of its use of "foreignness" to justify its surveillance, whether or not the facts support that characterization.

CONCLUSION

By generalizing about a complex area of law, one may view the rules pertaining to electronic surveillance as maintaining a virtual border between members of the national community who benefit from the protections of the Fourth Amendment and foreigners who do not. Benefits of full Fourth Amendment protections include the rigorous judicial review enunciated in *Berger* and codified in the Wiretap Act. Under those requirements, a judge conducts substantial oversight of executive branch surveillance before, during and after an investigation. Because of the inability of purely physical borders to separate those protected by the procedural requirements from those not so protected, electronic surveillance law determines when foreign persons acquire Fourth Amendment protections and when U.S. Persons lose them. The laws are designed to ensure that U.S. Persons will not be found to sacrifice the full protections of the Fourth Amendment until the government has established to a special court that the targeted person is an

Amendments Act).

[155] *See* FISA Amendments Act § 802.

[156] *See, e.g.*, Hepting v. AT & T Corp., 439 F. Supp. 2d 974, 992-94 (N.D. Cal. 2006) (denying government's claim that the states secrets privilege categorically barred an action accusing the defendant of violating plaintiffs' constitutional and statutory rights by assisting the NSA in the TSP).

agent of a foreign power based on more than just First Amendment protected activities. To the extent the laws permit the executive to exile without sufficient justification, oversight, and accountability, they should be fixed.