

# DISAPPEARING SAFEGUARDS: FISA NONRESIDENT ALIEN “LOOPHOLE” IS UNCONSTITUTIONAL

*Brenton Hund*

## TABLE OF CONTENTS

I. INTRODUCTION .....	169	R
II. BACKGROUND – WARRANTLESS SURVEILLANCE .....	174	R
A. Early Wiretapping Cases and Statutes .....	174	R
B. FISA Basics .....	180	R
1. The FISA Probable Cause Standard .....	182	R
2. The “Purpose” Provision .....	184	R
3. The “Wall” and Lack of Information-Sharing Between the Criminal Division and the FBI .....	187	R
C. Amendments to FISA .....	190	R
1. The Patriot Act .....	190	R
2. The “Lone Wolf” Amendment .....	200	R
3. USA PATRIOT Improvement and Reauthorization Act of 2005 .....	201	R
III. THE NONRESIDENT ALIEN “LOOPHOLE” SHOULD BE REEXAMINED .....	202	R
A. Congress Purposefully Created a Dichotomy Between U.S. Persons and Nonresident Aliens ...	204	R
B. United States v. Duggan and Circumventing the FISA Requirements .....	206	R
C. The Disappearing Nonresident Alien Safeguards .....	210	R
D. Adding Up the FISA Amendments .....	212	R
E. Constitutional Concerns .....	215	R
F. Possible Remedies .....	218	R
IV. CONCLUSION .....	221	R

### I. INTRODUCTION

The history and law related to conducting electronic surveillance and protecting national security have evolved from a tension

between the competing demands of the President and the public.<sup>1</sup> Whereas the Executive is enabled and required by the Constitution to gather intelligence information for the preservation of the nation,<sup>2</sup> the American public is protected by the Fourth Amendment which sets boundaries on the scope of unreasonable searches and seizures.<sup>3</sup> It is upon this backdrop in 1978 that the Foreign Intelligence Surveillance Act (FISA)<sup>4</sup> was enacted; its purpose was to strike a calculated balance between advancing the government's national security interests on the one hand, and protecting an individual citizen's rights and liberties on the other.<sup>5</sup>

While one set of national security law standards has developed to balance the tension between the citizen public and the national government, another set of national security law standards has developed with respect to "nonresident aliens."<sup>6</sup> Not surprisingly, this second set of standards has always tipped decidedly in favor of the government.<sup>7</sup> FISA codified this dichotomy by applying one

---

<sup>1</sup> H.R. REP. NO. 95-1283, pt. 1, at 15 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf> (President's powers to gather intelligence and the requirements of the Fourth Amendment are "competing demands.").

<sup>2</sup> See U.S. CONST. art. II, § 1, cl. 8 ("Oath Clause"). See also *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 310 (1967).

<sup>3</sup> See U.S. CONST. amend. IV (providing that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . .").

<sup>4</sup> Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as 50 U.S.C. §§ 1801-1811 (1978)) [hereinafter Original FISA 1978]. FISA has been amended numerous times since 1978 and, as codified today, it runs from 50 U.S.C. §§ 1801-1871.

<sup>5</sup> The Senate Judiciary Committee report that accompanied the enactment of FISA explained the need for the legislation:

The committee believes that the Executive Branch of Government should have, under proper circumstances and with appropriate safeguards, authority to acquire important foreign intelligence information by means of electronic surveillance. The committee also believes that the past record and the state of the law in the area make it desirable that the Executive Branch not be the sole or final arbiter of when such proper circumstances exist. *[FISA] is designed to permit the Government to gather necessary foreign intelligence information by means of electronic surveillance but under limitations and according to procedural guidelines which will better safeguard the rights of individuals.*

S. REP. NO. 95-604, at 9 (1978) (emphasis added).

<sup>6</sup> Nonresident aliens are "aliens in the United States who are tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel, illegal aliens, etc." See H.R. REP. NO. 95-1283. See *infra* note 198 and accompanying text.

<sup>7</sup> See, e.g., S. REP. NO. 95-604, at 21 ("[This] bill establishes a different standard for illegal aliens and foreign visitors.").

set of rules to United States persons<sup>8</sup> and another, greatly relaxed set of rules to nonresident aliens.<sup>9</sup> Under FISA today, the government has virtually unrestricted, unchecked power in wiretapping and searching nonresident aliens.<sup>10</sup>

In the committee hearings prior to FISA's enactment, the government provided an explanation for relaxing the requirements on targeting nonresident aliens under FISA. The government was able to demonstrate a legitimate need to be able to target nonresident aliens promptly and without undue encumbrance.<sup>11</sup> Legislative findings showed, for example, that a significant number of Soviet exchange students were found to be intelligence officers and that large numbers of temporary aliens who visited the United States were working for foreign intelligence networks.<sup>12</sup> Congress determined that nonresident aliens, as compared to United States persons, were more likely to be officers of a foreign power, more likely to be sources of foreign intelligence information, and more likely to be visiting the United States for a limited time, and therefore it was reasonable to create a dichotomy between the two groups.<sup>13</sup> It is because of this dichotomy that the government may conduct FISA surveillance on nonresident aliens at a different and much lower standard than that required for conducting FISA surveillance on United States persons.<sup>14</sup>

---

<sup>8</sup> The term "United States person" is a term of art used in FISA which includes by definition "United States citizens and permanent resident aliens." See Original FISA 1978 § 101(i) (codified at 50 U.S.C. § 1801(i) —current version same as original) (defining United States person). By definition, the classes "United States person" and "nonresident alien" are mutually exclusive. See *infra* note 201 and accompanying text.

<sup>9</sup> See discussion *infra* Part III.

<sup>10</sup> See discussion *infra* Part III.

<sup>11</sup> See H.R. REP. NO. 95-1283, pt. 1, at 33-34.

With respect to those nonresident aliens . . . th[e government's] need [to be able to obtain FISA warrants under relaxed standards] has been demonstrated to this committee in testimony before it. . . . The Committee finds ample evidence that non-resident aliens who act in the United States as officers, members, or employees of a foreign power are likely sources of foreign intelligence or counterintelligence information.

*Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.* at 20 (stating that "it is presumed that nonresident aliens who are officers or employees of a foreign power are likely sources of foreign intelligence information" and "this standard [which differentiates between United States persons and nonresident aliens] is considered by the Committee to be reasonable").

<sup>14</sup> See *infra* Part III.A for a complete discussion of the reduced standards enacted for surveillance against nonresident aliens.

Various constitutional issues emerged from the creation of this dichotomy,<sup>15</sup> but Congress concluded that the alienage distinctions fully complied with the Constitution.<sup>16</sup> Congress deemed the class of nonresident aliens “limited”<sup>17</sup> and the distinctions “reasonable.”<sup>18</sup> Nevertheless, constitutional challenges to the reduced standard followed. For example, in several criminal cases which postdated the enactment of FISA, the government used information acquired from nonresident alien wiretaps to prosecute United States persons.<sup>19</sup> The defendants in these cases, United States persons, argued that the government circumvented FISA requirements by targeting nonresident aliens under the reduced standard, only to eventually bring charges against a United States person. The courts dismissed this argument and held that incidental information collected on a wiretap *could legally be used against a United States person*.<sup>20</sup> In other words, the government had successfully found a loophole in which it could obtain incriminating evidence against a United States person without adhering to any of the safeguards imposed for such surveillance.

The “nonresident alien loophole,” as it will be termed in this note, exists as a result of the dichotomy created between United States persons and nonresident aliens under FISA. When the government for whatever reason cannot meet the minimum requirements for targeting a United States person under FISA, it is free to obtain FISA surveillance authorization on a nonresident alien—perhaps someone close to the desired United States person—under greatly reduced standards, and all incidental incriminating evidence obtained against the desired United States person (i.e. eavesdropping evidence, evidence derived from physical searches, etc.) is admissible as secret evidence in a criminal prosecution against the desired United States person. In other words, the gov-

---

<sup>15</sup> See, e.g., H.R. REP. NO. 95-1283, pt. 1, at 33 (“Some have questioned whether it is constitutional to treat nonresident aliens differently from United States citizens . . . either because the nonresident aliens’ fourth amendment rights are violated or because to deny them protections afforded U.S. citizens denies them equal protection under the laws.”).

<sup>16</sup> *Id.*

<sup>17</sup> *Id.* at 32 (stating that nonresident aliens are “limited to aliens in the United States who are tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel, illegal aliens, etc”).

<sup>18</sup> See *supra* note 13.

<sup>19</sup> See, e.g., *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

<sup>20</sup> See *infra* note 221.

ernment has an available work-around for targeting United States persons by utilizing the nonresident alien loophole.

At one point the loophole was very narrow. Safeguards and restrictions in 1978 confined the loophole to a limited number of situations and circumstances.<sup>21</sup> However, amendments in the late 1990s and early 2000s, including the USA Patriot Act<sup>22</sup> and the Lone Wolf Amendment,<sup>23</sup> not only greatly expanded the government's powers to combat terrorist threats, but also expanded the once narrow class of targets reached by the nonresident alien loophole.<sup>24</sup> Perhaps the erosion of the nonresident alien requirements was merely an unintended side-effect of otherwise well-intentioned legislation to update the government's counterterrorism capabilities. In any event, the ultimate outcome has been that the once very narrowly-constrained nonresident alien loophole has been expanded significantly and the potential for abuse against United States persons has increased proportionately.<sup>25</sup>

The purpose of this note is to expose the dangerous threats against United States persons resulting from the erosion of important nonresident alien safeguards. This note does not challenge the disparate treatment of United States persons and nonresident aliens under the original FISA as enacted in 1978, but questions the subsequent removal of the substantive safeguards originally imposed on nonresident alien wiretapping. The nonresident alien loophole has been expanded beyond any possible original vision of Congress.<sup>26</sup> When Congress enacted FISA in 1978, the government was allowed to seek a FISA warrant only if it could demonstrate that its primary purpose was intelligence gathering, *not* criminal prosecution. At the time of enactment, the government was also required to prove a nexus between the target and a foreign power. By contrast, today, both of these fundamental require-

---

<sup>21</sup> See *infra* note 272.

<sup>22</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, §§ 206–208, 214, 215, 218, 504, 1003, 115 Stat. 272, 282, 283, 286, 291, 364, 392 (2001) (codified as amended at 50 U.S.C. §§ 1805(c)(2)(B), 1805(e)(1), 1824(d), 1803(a), 1805(f), 1842, 1843, 1861, 1862, 1804(a)(7)(B), 1806(k), 1825(k), 1801(f)(2) (2001)) [hereinafter Patriot Act].

<sup>23</sup> Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004) (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2004)) [hereinafter Lone Wolf Amendment].

<sup>24</sup> See *infra* Part III.D.

<sup>25</sup> See *infra* Part III.

<sup>26</sup> See *infra* Part III.

ments have been repealed. All that remains to safeguard an unsuspecting public from nonresident alien wiretapping abuses is a mere filing requirement.<sup>27</sup>

Part I will explore the complex background and history of FISA, an understanding of which is essential to a complete examination of the nonresident alien loophole. Part II will examine (a) early wiretapping cases, statutes and events; (b) the FISA probable cause standard, the “purpose” provision, and the so-called “wall” between the criminal division and the FBI; and (c) three critical amendments to FISA: the Patriot Act, the Lone Wolf Amendment and the USA Patriot Improvement and Reauthorization Act of 2005.

Part III will discuss in further detail the nonresident alien loophole, the dichotomy between nonresident aliens and United States persons, disappearing safeguards, and constitutional problems that have been overlooked. Part III will also examine possible solutions and remedies which would raise the loophole back up to constitutional par.

Finally, Part IV will conclude with the proposition that, as it currently stands, the nonresident alien loophole is unconstitutional and requires legislative attention. Until such legislative action is taken United States persons will remain threatened by the government’s ability to exploit the loophole.

## II. BACKGROUND—WARRANTLESS SURVEILLANCE

### A. *Early Wiretapping Cases and Statutes*

Executive wiretapping authority is vested in the Oath Clause of Article II of the Constitution, which confers upon the President the responsibility to “preserve, protect and defend the Constitution.”<sup>28</sup> The clause has been interpreted to give the President con-

---

<sup>27</sup> See *infra* notes 245–248 and accompanying text.

<sup>28</sup> U.S. CONST. art. II, § 1, cl. 8. The Supreme Court interpreted this oath of office as imposing a presidential obligation to “protect our Government against those who would subvert or overthrow it by unlawful means.” *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 310 (1967). The Senate reported in 1978 that, over the years, the Executive had made broad use of its wiretapping powers, and stated that “every President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority.” S. REP. NO. 95-604, at 7 (1978). Although many cite the Nixon Administration’s extensive use of presidential wiretapping power as an aberration, the Senate concluded that such wiretapping by the executive had actually been more the historical norm. *Id.* The Senate found that “[w]hile the number of illegal or improper national security taps and bugs conducted during the Nixon Administration may have ex-

siderable latitude in conducting affairs relating to national security.<sup>29</sup> Although the Supreme Court has never expressly weighed in on whether the Executive may conduct *warrantless* surveillance, courts and Congress have consistently shown extraordinary deference to the Executive in matters concerning national security.<sup>30</sup>

---

ceeded those in previous administrations, the surveillances were regrettably by no means atypical.” *Id.* In other words, use of Executive wiretapping—even abusive use of Executive wiretapping—was nothing new, even in the 1970s.

<sup>29</sup> See *infra* note 30.

<sup>30</sup> See, e.g., H.R. REP. NO. 95-1283, pt. 1, at 15–21 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf> (chronicling the history of wiretapping, showing a reluctance by Congress and the courts to intervene against the President on national security matters). What is now a heavily debated issue in 2007—determining the constitutional limits on the President’s authority to wiretap—was also an open question in 1978. To that question, the Congress could only conclude that the limits on the President’s constitutional power to conduct warrantless surveillance had not been established. *Id.* at 20–21 (“[A]fter almost 50 years of case law dealing with the subject of warrantless electronic surveillance, and despite the practice of warrantless foreign intelligence surveillance sanctioned and engaged in by nine administrations, constitutional limits on the President’s powers to order such surveillances remains an open question.”). In response to FISA, the first enacted legislation to ever regulate the use of electronic surveillance for foreign intelligence purposes, S. REP. NO. 95-604, at 7, the Executive defended its constitutional authority and refuted any notion that its inherent powers could be curtailed by a congressional act. In 1978, Attorney General Griffin Bell explained the Carter Administration’s position. “[FISA] recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that this does not take away the power of the President under the Constitution.” See *Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence*, 95th Cong. 15 (1978) (testimony of Attorney General Griffin Bell), quoted in H.R. REP. NO. 109-384, at 14 (2006).

Before FISA, warrantless wiretapping withstood constitutional challenge, so long as the purpose was for gathering foreign intelligence. See, e.g., *United States v. Butenko*, 494 F.2d 593, 601 (3d Cir. 1974) (en banc) (holding that warrantless wiretaps were constitutional where the surveillance was “conducted and maintained solely for the purpose of gathering foreign intelligence information”); *United States v. Brown*, 484 F.2d 418, 420–21 (3d Cir. 1973) (upholding a conviction based on evidence collected by warrantless wiretaps where the surveillance was “for the purpose of gathering foreign intelligence”). The carve-out for national security illuminated an important distinction between criminal investigations, which were subject to the traditional warrant requirements and judicial scrutiny, and intelligence investigations, which were granted extraordinary deference. See, e.g., S. REP. NO. 90-1097, at 94 (1968) (recognizing “a distinction between the administration of domestic criminal legislation . . . and the conduct of foreign affairs”). See also *infra* notes 31–42 and accompanying text.

In 2005 and 2006 public debate on warrantless wiretapping reached a crescendo after the New York Times exposed a secret Terrorist Surveillance Program conducted by the National Security Agency (NSA) and sanctioned by the Bush administration. See James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. The debate was, and still is, over whether and to what extent the President

R

R

may lawfully bypass FISA to conduct unauthorized surveillance in the name of national security. Some argue that the Executive retains the inherent authority to protect and defend the nation under his Oath of office and Congress may not impede this constitutional right and responsibility. For example, Syracuse University College of Law Professor William Banks, a leading authority on FISA, explained that the President possessed inherent warrantless wiretapping powers and that he could make use of these powers absent congressional or judicial approval. See William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1157 n.41 (2003).

Congress cannot legislate to deny surveillance authority that is part of a core Article II power of the executive. While the executive branch has worked within FISA for 25 years, it remains possible that new threats or conditions could give rise to renewed claims for warrantless executive branch surveillance authority.

*Id.*

The Foreign Intelligence Surveillance Court of Review (FISCR) also stated affirmatively that the President possesses inherent wiretapping powers. See *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. . . . *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.*

*Id.* (emphasis added). Those “other courts” which have upheld warrantless electronic surveillance conducted for a foreign intelligence purpose include the Third, Fourth, Fifth, and Ninth Circuits. See *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (“[V]irtually every court that had addressed the issue had concluded that the President had the inherent power to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment.”). Because the Supreme Court has never expressly weighed in on whether the President has the inherent authority to conduct warrantless wiretaps, see, e.g., Supp. Brief for United States at Part I(A), *In re Sealed Case*, 310 F.3d 717, the FISCR’s approval of the inherent powers argument is currently the highest legal pronouncement on the issue.

Those in opposition to the argument that the Executive possesses the exclusive ability to conduct warrantless wiretapping counter with a different constitutional argument. They argue that the Constitution clearly confers the power to conduct national security surveillance on *both* the President *and* Congress together.

Foreign intelligence collection is not among Congress’s powers enumerated in Article I of the Constitution, nor is it expressly mentioned in Article II as a responsibility of the President. Yet it is difficult to imagine that the Framers intended to reserve foreign intelligence collection to the states or to deny the authority to the federal government altogether. It is more likely that the power to collect intelligence resides somewhere within the domain of the foreign affairs and war powers, both of which areas are inhabited to some degree by the President *together with the Congress*.

Memorandum on the Subject of Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information from Elizabeth B. Bazan & Jennifer K. Elsea, Cong. Research Serv. Legislative Attorneys, American Law Division 4 (Jan. 5, 2006) (emphasis added), <http://www.fas.org/sgp/crs/intel/m010506.pdf>. The memo continues by citing numerous sections of the Constitution to support the argument that the framers intended wiretapping powers to be shared by the executive and legislative branches together.

Federal wiretapping jurisprudence debuted in 1928 with *Olmstead v. United States*.<sup>31</sup> The Supreme Court held that the interception of a suspected bootlegger's phone conversations did not amount to "seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage.'" <sup>32</sup> Because there was no physical trespass, the Court held that Roy Olmstead's Fourth Amendment search and seizure rights were not violated.<sup>33</sup>

Congress reacted to the *Olmstead* decision by enacting the Federal Communications Act of 1934, which imposed the first legislative restrictions on wiretapping. However, the restrictions only pertained to domestic wiretaps, leaving wiretaps of a national security nature untouched by the legislation. In the 1950s, the FBI expanded their warrantless surveillance activities in order to assist in uncovering Soviet intelligence operatives and Communist leaders.<sup>34</sup> The FBI found neither the courts nor Congress were willing to contest wiretapping authority that was framed in a national security context.

In 1965, the President self-imposed a safeguard that required the Attorney General to sign off on counterintelligence surveillance measures.<sup>35</sup> This requirement of authorization infused a level of accountability into national security-related wiretapping directives where, previously, there had been none.

---

The Constitution specifically gives to Congress the power to "provide for the common Defense," 11 U.S. CONST. art. I, § 8, cl. 1; to "declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water," *id.* § 8, cl. 11; "To raise and support Armies," and "To provide and maintain a Navy," *id.* § 8, cls. 12–13; "To make Rules for the Government and Regulation of the land and naval Forces," *id.* § 8, cl. 14, "To declare War," *id.* § 8, cl. 1[1]; and to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof," *id.* § 8, cl. 18. The President is responsible for "tak[ing] Care that the Laws [are] faithfully executed," Art. II, § 3, and serves as the Commander-in-Chief of the Army and Navy, *id.* § 2, cl. 1.

*Id.* at 4 n.11. Thus, this argument infers from the constitutional provisions cited that because the powers of defense and national security were granted to both the Legislature and the Executive, wiretapping authority is also shared between the two branches.

<sup>31</sup> *Olmstead v. United States*, 277 U.S. 438 (1928).

<sup>32</sup> *Id.* at 466.

<sup>33</sup> *Id.*

<sup>34</sup> See H.R. REP. NO. 95-1283, pt. 1, at 16 (citing Memorandum from J. Edgar Hoover, FBI Director, to Deputy Attorney General (May 4, 1961)).

<sup>35</sup> Supp. Brief of Respondent, *Black v. United States*, 385 U.S. 26 (1966), quoted in H.R. REP. NO. 95-1283, pt. 1, at 17 ("The specific authorization of the Attorney General must be obtained in each instance when [the national security] exception is invoked.").

In 1967, the Supreme Court in *Katz v. United States* reversed the *Olmstead* doctrine, holding that a “bug” placed on the outside of a public telephone booth violated the defendant’s reasonable expectation of privacy as protected by the Fourth Amendment.<sup>36</sup> Thus, a physical trespass was no longer required to implicate a Fourth Amendment violation.<sup>37</sup> However, the Court was careful to expressly abstain from extending its holding to cases involving national security.<sup>38</sup>

The Supreme Court dealt a blow to the Executive in 1972 in what is commonly referred to as the *Keith* case, which involved a domestic organization’s plan to bomb a CIA office in Michigan. The Court held that in cases involving domestic national security, the federal government would not be permitted to conduct surveillance without prior judicial authority.<sup>39</sup> In *Keith*, the Court introduced an important principle that flexible or differing standards—i.e. one standard for counterintelligence, and another for criminal—could coexist under the Fourth Amendment.<sup>40</sup> The Court stated that “[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.”<sup>41</sup> The concept of flexible standards would prove important to FISA, in which the probable cause requirement for securing a warrant for counterintelligence diverges from the criminal equivalent.<sup>42</sup>

Pressures to regulate foreign intelligence surveillance increased in the 1970s. Congress in 1973 made the first of several

---

<sup>36</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>37</sup> Under the *Olmstead* doctrine, unless a physical trespass was present (i.e. “bugging” typically required a physical trespass, while wiretapping did not), no federal constitutional Fourth Amendment issue was raised. See *Olmstead*, 277 U.S. at 466.

<sup>38</sup> *Katz*, 389 U.S. at 358 n.23 (stating that situations involving national security are “not presented by this case”).

<sup>39</sup> *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1967). The district court judge who first presided over the case was Damon J. Keith, and the case is typically referred to simply by his last name, Keith. For purely domestic wiretapping, not implicating a foreign power, the Court required the Executive to obtain a traditional Title III criminal warrant. *Id.* at 323–24. In other words, *Keith* limited the national security exception (which otherwise gave the Executive essentially unchecked wiretapping authority) to matters that implicated a foreign power.

<sup>40</sup> *Id.* at 322–23 (determining that one standard for a criminal warrant and another standard for a counterintelligence warrant could coexist under the Fourth Amendment).

<sup>41</sup> *Id.*

<sup>42</sup> See discussion *infra* Part II.B.1, comparing and contrasting the FISA and criminal probable cause standards.

attempts to pass legislation that would regulate this surveillance.<sup>43</sup> The Nixon Administration opposed the legislation, and Henry Peterson, the Assistant Attorney General, offered this sentiment to the House Judiciary Committee on behalf of the Administration: “[L]et me be very brief. We oppose these bills. That is it.”<sup>44</sup> The Nixon Administration, of course, is most notably known for its flagrant abuse of wiretapping privileges in the Watergate scandal.<sup>45</sup> These abuses, and others involving the CIA, FBI, and NSA were uncovered and disclosed in a report by the late Senator Frank Church of Idaho.<sup>46</sup> Because of increasing political pressures and also because of fears that the judiciary would incrementally continue to encroach on wiretapping powers,<sup>47</sup> the Executive became more amenable to working with Congress on wiretapping legisla-

---

<sup>43</sup> See H.R. REP. NO. 95-1283, pt. 1, at 13 (1978), available at <http://www.cnss.org/rpt%20951283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf>.

<sup>44</sup> *Id.*

<sup>45</sup> See S. REP. NO. 95-604, at 7 (1978) (stating that abuses in electronic surveillance “were initially illuminated in 1973 during the investigation of the Watergate break-in”).

<sup>46</sup> See S. REP. NO. 95-701, at 9 (1978) (stating that the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) “provided firm evidence that foreign intelligence electronic surveillance involved abuses and that checks upon the exercise of those clandestine methods were clearly necessary”). The Church Committee found abuses in executive branch investigations of civil rights leaders, Vietnam protestors, and African-American rights advocates. See S. REP. NO. 95-604, at 8. Additionally, the Church Committee found that

[s]ince the 1930’s, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group.

*Id.*

<sup>47</sup> See, e.g., Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL’Y 319, 334 (2005) (“Zweibon led the Department of Justice to fear that the D.C. Circuit would invalidate all warrantless electronic surveillance for foreign intelligence information.”). In *Zweibon v. Mitchell*, 516 F.2d 594, 613–614 (D.C. Cir. 1975) (en banc), the Jewish Defense League (JDL) successfully challenged the legality of secret wiretaps on the grounds that no national security issue was implicated. The government argued unsuccessfully that since JDL activities threatened to provoke a hostile response from the Soviet Union, those actions constituted a threat to national security and fell within the national security exception for executive wiretapping. *Id.* The Executive branch was concerned because the court had been able to construe the national security exception narrowly and invalidate the wiretapping. Because the Executive branch feared further judicial encroachment into its wiretapping power, rather than passively wait for the court to act, the Executive, specifically the Department of Justice, decided to collaborate with Congress on writing FISA legislation which would regulate the issuing of warrants for foreign intelligence surveillance.

tion. In 1976, the Ford Administration took the revolutionary step of supporting legislation that would impose judicial oversight into foreign intelligence surveillance. The stage was set for FISA.

### B. *FISA Basics*

In 1978, Congress passed FISA, which established standards for obtaining a court order authorizing national security intelligence investigations.<sup>48</sup> FISA was enacted in order to provide a “secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this nation’s commitment to privacy and individual rights.”<sup>49</sup> Through FISA, the Foreign Intelligence Surveillance Court (FISC) was created, which today consists of eleven judges appointed by the Chief Justice of the Supreme Court.<sup>50</sup> Also created was an appellate court, the Foreign Intelligence Sur-

---

<sup>48</sup> Original FISA 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as 50 U.S.C. §§ 1801–1811 (1978)). FISA legislation was the first of its kind. Congress reported that “[t]he Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States for foreign intelligence purposes.” S. REP. NO. 95-604, at 7. Its need was based on “abuses of domestic national security surveillances [that] have been disclosed.” H.R. REP. NO. 95-1283, pt. 1, at 21. Dissenters to FISA argued that the Act would improperly subject political decisions to judicial intrusion. H.R. REP. NO. 95-1283, Dissenting Views on H.R. 7308, pt. 1, at 111. The dissenters quoted Justice Jackson’s 1948 Supreme Court decision in opposition to FISA legislation. Justice Jackson wrote:

The President, both as Commander-in-Chief and as the Nation’s organ for foreign affairs, has available intelligence services whose reports are nor ought not to be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret. Nor can courts sit in camera in order to be taken into executive confidences. But even if courts could require full disclosure, the very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy. They are and should be undertaken only by those directly responsible to the people whose welfare they advance or imperil. They are decisions of a kind for which the Judiciary has neither aptitude, facilities nor responsibility and which has long been held to belong in the domain of political power not subject to judicial intrusion or inquiry.

*Id.* (quoting *Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.*, 333 U.S. 103, 111 (1948) (citations omitted)).

<sup>49</sup> S. REP. NO. 95-604, at 15.

<sup>50</sup> The original FISC consisted of only seven judges. See Original FISA 1978 § 103(a) (codified as amended at 50 U.S.C. § 1803(a) (1978)). The number was increased to eleven in 2001 with the passage of the Patriot Act. See Patriot Act, Pub. L. No. 107-56, § 207, 115 Stat. 272, 282 (2001) (codified as 50 U.S.C. § 1803(a) (2001)). The FISC is known as a

veillance Court of Review (FISCR), which has jurisdiction to review denials of FISA applications by the FISC.<sup>51</sup> The United States Supreme Court has the theoretical final word,<sup>52</sup> although to date no applications for certiorari to the Supreme Court have been made.

The process for obtaining a FISA warrant begins with an application, which must first be approved by the Attorney General. The application is submitted to the FISC by a federal officer.<sup>53</sup> The application must contain (1) the identity, if known, of the target;<sup>54</sup> (2) information relied on by the government to illustrate that the target is a “foreign power” or an “agent of a foreign power”;<sup>55</sup> (3) evidence that the facility targeted for the electronic surveillance is currently being used, or is about to be used, by the foreign power or its agent;<sup>56</sup> (4) an explanation of the minimization procedures to be used;<sup>57</sup> (5) a description of the nature of the information that is sought to be collected;<sup>58</sup> and (6) certification by a high level executive branch official “employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate” that “a significant purpose” of the FISA application is to “obtain foreign intelligence information.”<sup>59</sup> Additionally, before the application may be granted, the FISC must also determine whether there is “probable cause to believe

---

“secret court” because its proceedings are classified and sealed. Only two opinions in its twenty-eight-year history have been made public.

<sup>51</sup> See 50 U.S.C. § 1803(b) (2006). There has only been one appeal in the history of FISA to the FISCR. See discussion *infra* Part II.C.1.b.

<sup>52</sup> See § 1803(b).

<sup>53</sup> 50 U.S.C. § 1804(a) (2006).

<sup>54</sup> § 1804(a)(3).

<sup>55</sup> § 1804(a)(4)(A). Congress recently passed the Lone Wolf Amendment to FISA, which added a provision enabling the FBI to pursue certain targets who act independently of a foreign power. Such targets who do not satisfy the “agent of a foreign power” provision may now be targeted under FISA so long as they “engage[ ] in international terrorism or activities in preparation therefore [sic].” See Lone Wolf Amendment, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004) (codified as 50 U.S.C. § 1801(b)(1)(C) (2004)); 50 U.S.C. § 1804(c) (defining “international terrorism”). See also discussion *infra* Part II.C.2.

<sup>56</sup> See § 1804(a)(4)(B).

<sup>57</sup> § 1804(a)(5)(A). Minimization procedures are imposed on government investigators that require them to “minimize the acquisition and retention, and prohibit the dissemination” of information collected that does not have foreign intelligence value. 50 U.S.C. § 1801(h) (2006).

<sup>58</sup> § 1804(a)(6).

<sup>59</sup> § 1804(a)(7). See *infra* Part II.B.2.

that the target of the search or surveillance is a foreign power or agent of a foreign power.”<sup>60</sup>

### 1. *The FISA Probable Cause Standard*

The FISA probable cause standard has historically been a source of some confusion. Criminal probable cause requires that a person “is committing, has committed, or is about to commit a [Title III crime]”<sup>61</sup> whereas FISA sets forth a probable cause requirement that the target is a “foreign power” or an “agent of a foreign power.”<sup>62</sup> On the one hand, the Department of Justice (DOJ) stated that “FISA imposes a more relaxed criminal probable cause standard than Title III.”<sup>63</sup> On the other hand, the FBI was later criticized for holding an unnecessarily high standard for probable cause under FISA.<sup>64</sup> Some argue that probable cause under FISA is unconstitutional and lacks meaningful standards.<sup>65</sup> Others argue that obtaining a FISA warrant is more difficult than obtaining a criminal warrant.<sup>66</sup>

---

<sup>60</sup> 50 U.S.C. § 1805(a)(3)(A) (2006).

<sup>61</sup> Supp. Brief for United States as App. pt. 2, *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). “Title III crime” refers to the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (codified as amended at 18 U.S.C. §§ 2501–2522 (2006)) [hereinafter Title III].

<sup>62</sup> 50 U.S.C. § 1801(b)(2) (2006). FISA’s probable cause requirement is rooted in criminal conduct, and includes a “may involve” or “about to involve” standard that relates to violations of criminal statutes. § 1801(b)(2) The probable cause requirement only pertains to United States persons, not nonresident aliens. § 1801(b)(2)(B). For more information on the distinctions made for nonresident aliens, see discussion on nonresident alien loophole *infra* Part III.

<sup>63</sup> See Supp. Brief for United States, *supra* note 61.

<sup>64</sup> S. REP. NO. 108-40, at 36 (2003).

<sup>65</sup> See, e.g., Amici Brief at 13, *In re Sealed Case*, 310 F.3d 717 (arguing that “FISA . . . orders require only probable cause to believe that the target is a foreign power or agent thereof” and “do *not* require probable cause to believe that the target is engaging in criminal activity”) (emphasis in original). Amici argued that the significantly greater latitude, in terms of surveillance, that is afforded the Executive under FISA, as compared to Title III, results in FISA falling short of constitutional minimums. *Id.* Since FISA holds *ex parte* proceedings, where the government is the only party, the FISCR accepted briefs filed by the American Civil Liberties Union (ACLU) and the National Association of Criminal Defense Lawyers (NACDL) as *amici curiae*. See *In re Sealed Case*, 310 F.3d at 719.

<sup>66</sup> See Craig S. Lerner, *The USA Patriot Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 503 n.62 (2003).

At least judged by the number of bureaucratic hoops to jump through, a FISA warrant is harder to obtain than a garden-variety warrant. Whereas police officers can ordinarily secure law enforcement warrants in a manner of hours, the FISA application process, involving the highest levels of the Department of

The FISCER concluded that the FISA probable cause standard and the Title III criminal standard are basically the same.<sup>67</sup> The court stated that “while Title III contains some protections that are not in FISA, in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections.”<sup>68</sup> The FISCER also noted that “few of those differences have any constitutional relevance.”<sup>69</sup>

The Senate concurred and stated formally in 2003 that the FISA standard was not divergent from the criminal standard, but analogous to it.<sup>70</sup> In a report attached to the Lone Wolf Amendment to FISA,<sup>71</sup> the Senate concluded that “both FBI agents and FBI attorneys do not have a clear understanding of the legal standard for probable cause, as defined by the Supreme Court in the case of *Illinois v. Gates*.”<sup>72</sup> Perhaps caused by prosecutorial “risk-averseness, which is caused by ‘careerism,’”<sup>73</sup> or perhaps caused by judges “who may be imposing a higher standard than is required by law,”<sup>74</sup> the United States Attorney’s Office “regularly requir[ed] much more than probable cause before approving [FISA] affidavits (maybe, if quantified, 75 percent–80 percent probability and sometimes even higher).”<sup>75</sup> The Senate, quoting the 95th Congress from 1978, referred to the legislative history of FISA which showed unequivocally that the probable cause standard for FISA applications was to be the same as that used for obtaining criminal warrants: “In determining whether probable cause exists under [FISA], the court

---

Justice, as well as FBI or CIA, bureaucracy, generally takes weeks or even months.

*Id.* In practice, the FISA request would initially be reviewed by the Office of Intelligence and Policy Review (OIPR), then sent to the director of the FBI for certification, forwarded to the Attorney General for approval, and finally scheduled on the docket of the FISC. *Id.* at 503.

<sup>67</sup> See *In re Sealed Case*, 310 F.3d at 741.

<sup>68</sup> *Id.*

<sup>69</sup> *Id.* at 737.

<sup>70</sup> S. REP. NO. 108-40, at 37 (2003).

<sup>71</sup> See discussion on the Lone Wolf Amendment *infra* Part II.C.2.

<sup>72</sup> S. REP. NO. 108-40, at 35. In *Illinois v. Gates*, 462 U.S. 213, 236, 238 (1983), “probable cause” for criminal warrants requires an examination of “the totality-of-the-circumstances” and also that “there is a fair probability” that criminal conduct is occurring.

<sup>73</sup> S. REP. NO. 108-40, at 37 (citing *Oversight Hearing on Counterterrorism: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 226–27 (2002) (statement of Coleen Rowley, Special Agent), available at [http://www.fas.org/irp/congress/2003\\_rpt/srpt108-40.html](http://www.fas.org/irp/congress/2003_rpt/srpt108-40.html)).

<sup>74</sup> *Id.*

<sup>75</sup> S. REP. NO. 108-40, at 37 (quoting statements made in Letter from Coleen Rowley, Special Agent, to Robert S. Mueller, III, FBI Director 3 (May 21, 2002)).

must consider the same requisite elements which govern such determinations in the criminal context.”<sup>76</sup>

No probable cause standard is required when the government applies for a FISA warrant against nonresident aliens.<sup>77</sup> However, as will be discussed in Part III, if United States persons are targeted vicariously through aliens—i.e. a FISA application is made against a nonresident alien, but the intended target is a United States person closely associated with the alien—then the government has effectively circumvented the important and debated probable cause requirement altogether.

## 2. *The “Purpose” Provision*

FISA today requires that “a significant purpose” of the surveillance be for gathering foreign intelligence information. The original 1978 FISA required a much higher standard, “the purpose,” and there has been much debate over what this purpose provision actually required, and whether or not those requirements should have been relaxed.

The origins of the purpose provision controversy lie in the primary purpose test, a test which is most commonly attributed to the Fourth Circuit’s decision in 1980 in *United States v. Truong Dinh Hung*.<sup>78</sup> *Truong* was the first case to draw a sharp distinction between the dual purposes, criminal and foreign intelligence, of the government’s wiretapping investigations.<sup>79</sup> In scrutinizing the gov-

---

<sup>76</sup> *Id.* at 36 (citing S. REP. NO. 95-604, at 47 (1978)). It should be noted that when the 95th Congress made its statement, FISA warrants could only be obtained for electronic surveillance, not physical searches or pen register and trap and trace devices. S. REP. NO. 108-40, at 36 n.28. In addition, “[t]he FISA statute does not define ‘probable cause,’ although it is clear from the legislative history that Congress intended for this term to have a meaning analogous to that typically used in criminal contexts.” U.S. DEPARTMENT OF JUSTICE, FINAL REPORT OF THE ATTORNEY GENERAL’S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION 494 (May 2000) (Chapter 11, entitled “The Draft FISA Application: June 1997 to August 1997”), available at <http://www.loyola.edu/dept/politics/intel/lee-final-report.html> [hereinafter BELLOWS REPORT].

<sup>77</sup> See discussion on nonresident alien loophole *infra* Part III.

<sup>78</sup> See *United States v. Truong Dinh Hung*, 629 F.2d 908, 916 (4th Cir. 1980) (stating that the foreign intelligence exception to the warrant requirement applied only when the Executive “is attempting primarily to obtain foreign intelligence”). See also U.S. GENERAL ACCOUNTING OFFICE, REPORT NO. 01-780, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 13 n.16 (2001) [hereinafter GAO REPORT] (attributing the “judicially created primary purpose test” to *Truong*).

<sup>79</sup> *Truong*, 629 F.2d at 916 (stating that targets of government surveillance must “receive the protection of the warrant requirement if the government is primarily attempting

ernment's collection of evidence, the court held that only the evidence gathered primarily for foreign intelligence purposes was admissible.<sup>80</sup> The moment when the government shifted its investigative focus to a criminal prosecution, which was determined to be July 20, 1977, was the point after which all further evidence was deemed inadmissible and suppressed.<sup>81</sup> Thus, for any information to be admissible, the court required the government to show that its primary purpose for collecting such information was rooted in foreign intelligence.<sup>82</sup>

Several circuits adopted the *Truong* primary purpose test.<sup>83</sup> For example, in *United States v. Megahey*, a federal district court in New York acknowledged that while criminal prosecution was one outcome of a FISA warrant, the FISA surveillance was still appropriate “only if foreign intelligence surveillance is the Government’s primary purpose.”<sup>84</sup> The Second Circuit followed in *United States v. Duggan*, stating that “[t]he requirement that foreign intelligence information be the primary objective of the surveillance is plain” from the language of FISA.<sup>85</sup> In *United States v. Johnson*, the First Circuit concurred.<sup>86</sup> Acquiring evidence for a criminal prosecution

---

to put together a criminal prosecution”). The FISCR also stated that “the origin” of the “dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is *not*” came in *Truong*. *In re Sealed Case*, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (emphasis added).

<sup>80</sup> *Truong*, 629 F.2d at 915 (“[T]he executive should be excused from securing a warrant only when the surveillance is conducted ‘primarily’ for foreign intelligence reasons.”).

<sup>81</sup> *Id.* The *Truong* case was also unusual because it started in federal court before FISA was enacted, but was not decided until 1980, two years after FISA was passed. It follows, therefore, that FISA legislative history does not cite the *Truong* decision. When FISA passed in 1978, the statute incorporated a “purpose” provision, but made no specific mention of a “primary purpose” requirement anywhere in the act. FISA required that “the purpose” of the surveillance sought was to obtain “foreign intelligence information.” See Original FISA 1978 Pub. L. No. 95-511, §104(a)(7)(B), 92 Stat. 1783, 1789 (1978) (codified as amended at 50 U.S.C. § 1804(a)(7)(B) (1978)).

<sup>82</sup> *Truong*, 629 F.2d at 915.

<sup>83</sup> See *In re Sealed Case*, 310 F.3d at 726 (“Several circuits have followed *Truong* in applying similar versions of the ‘primary purpose’ test, despite the fact that *Truong* was not a FISA decision.”).

<sup>84</sup> *United States v. Megahey*, 553 F. Supp. 1180, 1189–90 (E.D.N.Y. 1982).

<sup>85</sup> *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984). The court cited requirements of § 1802(b) and § 1804 in support of the primary purpose test. *Id.*

<sup>86</sup> *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (“[A]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance.”) (citations omitted).

could not be a primary or sole purpose of a FISA investigation.<sup>87</sup> The primary purpose test imposed a standard that was demanding and required continued vigilance by the FBI in its FISA cases.

The primary purpose test ultimately served as a safeguard to protect against possible wiretapping abuses by the Executive. Perhaps that is why “[m]ost federal courts have adopted the primary purpose test in post-FISA cases.”<sup>88</sup> Without the primary purpose test, there were fears that criminal prosecutors could and would use FISA as an end run around Title III requirements.<sup>89</sup>

FISA was not created as another avenue for criminal prosecutors who grew tired of burdensome Title III requirements, or so that criminal prosecutors could indirectly control FBI investigations for their own purposes.<sup>90</sup> Information to be collected under the foreign intelligence exception before FISA, and under FISA after 1978, was always predicated on “legitimate electronic surveillance for foreign intelligence purposes.”<sup>91</sup> FISA was intended to help maintain a delicate balance between “our nation’s security on the one hand, and the preservation of basic human rights on the other.”<sup>92</sup>

Nevertheless, the primary purpose standard was officially abolished in the wake of the Patriot Act.<sup>93</sup> The shift toward a more

---

<sup>87</sup> Even still, since FISA was enacted in 1978, no court has ever used the primary purpose test to suppress evidence of criminal activity acquired under FISA. See Seamon & Gardner, *supra* note 47, at 366 (stating that “no court ever used *Truong’s* primary purpose test to suppress evidence acquired under the FISA”). Note that in *Truong*, the court *did* suppress evidence after July 20, 1977, the date when the FBI was deemed to have switched from an intelligence gathering objective to a criminal prosecution objective. However, *Truong* was not a FISA case in that the surveillance in question was entirely gathered before FISA was passed. Thus, *Truong* is excepted from the above statistic that no court has ever used the primary purpose test to suppress evidence under FISA.

<sup>88</sup> GAO REPORT, *supra* note 78, at 13.

<sup>89</sup> See *In re All Matters Submitted to the FISC*, 218 F. Supp. 2d 611, 624 (FISA Ct. 2002) (suggesting, for example, that with no primary purpose test “criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance)”).

<sup>90</sup> *Id.* (fearing that the Criminal Division would tell the FBI “what techniques to use, what information to look for, what information to keep as evidence and when use of the FISA can cease because there is enough evidence to arrest and prosecute.”).

<sup>91</sup> S. REP. NO. 95-604, at 15 (1978).

<sup>92</sup> *Id.* at 4 (quoting a statement made by President Jimmy Carter in announcing the FISA bill).

<sup>93</sup> Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291(2001) (*codified as amended at 50 U.S.C. 1804(a)(7)(B), 504 (2001)*). See also *In re Sealed Case*, 310 F.3d 717, 734 (FISA Ct. Rev. 2002) (stating succinctly that “the Patriot Act amendments clearly disapprove of the primary purpose test”).

R

R

lenient FISA was a response to the terrible tragedy of 9/11, and was intended to increase information sharing.<sup>94</sup> Information sharing, or lack thereof, was cited as a major contributor to the overall intelligence failure of 9/11.<sup>95</sup> Congress' solution was to eradicate this barrier through amending the purpose language. The result was not only increased communication, but also an expansive increase in the government's power to conduct foreign intelligence surveillance. A side effect of expanding the government's power was also to enlarge the nonresident alien loophole. Relaxing the requirements of the purpose provision now puts United States persons at a heightened risk of abuse.<sup>96</sup>

Part III of this note will discuss how the changes in FISA's purpose provision increased the government's powers of surveillance, and shifted the delicate balance between protecting national security on the one hand, and protecting individual privacy on the other, toward the former. Part III will also discuss how the Patriot Act's relaxing of "the purpose" to "a significant purpose" has helped widen the once very narrow nonresident alien loophole.

### 3. *The "Wall" and Lack of Information Sharing Between the Criminal Division and the FBI*

The lack of information sharing between the FBI and the Criminal Division was one of the major criticisms of the government in its failure to stop the 9/11 attacks.<sup>97</sup> The Patriot Act was passed in part to dispose of information sharing problems, and was also used to expand the Executive's ability to conduct foreign intel-

---

<sup>94</sup> For example, the benefit of changing the FISA language was to alleviate the FBI's continual fears of potential "(1) rejection of the FISA application or the loss of a FISA renewal and/or (2) suppression of evidence gathered using FISA tools" and take away the incentive for keeping valuable information secret. GAO REPORT, *supra* note 78, at 11. The "wall" (*see* discussion *infra* Part II.B.3), which was created by the primary purpose test and later dismantled by the Patriot Act, stifled communications between the FBI and the Criminal Division and gave rise to "a diminished level of coverage of suspected al-Qa'ida operatives in the United States." HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE AND THE SENATE SELECT COMM. ON INTELLIGENCE, REPORT OF THE JOINT INQUIRY INTO THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351 & H.R. REP. NO. 107-792, at xvii (2002) (pagination from unclassified version of report) [hereinafter REPORT OF THE JOINT INQUIRY].

<sup>95</sup> *See, e.g.*, RICHARD C. SHELBY, SEPTEMBER 11 AND THE IMPERATIVE OF REFORM IN THE U.S. INTELLIGENCE COMMUNITY, ADDITIONAL VIEWS OF SENATOR RICHARD C. SHELBY, VICE CHAIRMAN, SENATE SELECT COMM. ON INTELLIGENCE 49 (Dec. 10, 2002), [hereinafter SHELBY REPORT], available at <http://intelligence.senate.gov/shelby.pdf>.

<sup>96</sup> *See infra* Part III.

<sup>97</sup> *See, e.g.*, SHELBY REPORT, *supra* note 95.

ligence surveillance. The widening of the nonresident alien loophole—the major issue of this note—cannot be understood out of the context of the events which led to its widening. The basic sequence of events is as follows: (i) because of the primary purpose test, the DOJ erected a wall to protect itself; (ii) the erection of the wall led to information sharing problems; (iii) information sharing problems contributed significantly to the failures of 9/11; and (iv) 9/11 spawned a vigorous campaign to expand the government's ability to prevent such attacks in the future. The passage and implementation of the Patriot Act eliminated the primary purpose test, one of the two key provisions which limited and safeguarded non-resident alien surveillance.<sup>98</sup>

Because courts had been upholding the primary purpose test in cases like *Truong*, *Duggan*, and *Johnson*, the DOJ adopted procedures to comply with the primary purpose test and disseminated very conservative interpretations of these procedures, thus producing the problematic restrictive policy on information sharing.<sup>99</sup>

The DOJ's restrictive policies were not without justification. One of the principal events that led to the DOJ's restrictive policies on information sharing was the nearly botched 1994 investigation of Aldrich Ames. Ames, a CIA official, was arrested for spying for the Soviets.<sup>100</sup> The government had targeted Ames under FISA and much of the evidence that had been collected against him was the product of this FISA surveillance.<sup>101</sup> Although the government had a good case against Ames, Office of Intelligence and Policy Review (OIPR) head Richard Scruggs worried that FISA had been violated and the prosecution jeopardized because of significant coordination between the FBI and the Criminal

---

<sup>98</sup> See discussion *infra* Part III.C on disappearing safeguards.

<sup>99</sup> The DOJ was criticized for failing to understand the degree of information sharing permitted under FISA and for enacting procedures designed to avoid violating perceived constitutional requirements. Specifically, Office of Intelligence and Policy Review officials, the "gatekeepers" of information sharing between counterintelligence and the Criminal Division, maintained "an unduly strict interpretation of the primary purpose test," and were "overly cautious" in coordinating intelligence sharing. GAO REPORT, *supra* note 78, at 14.

<sup>100</sup> See *id.* at 13 ("Aldrich H. Ames, a Central Intelligence Agency official, was arrested on espionage charges of spying for the former Soviet Union and subsequently Russian intelligence.").

<sup>101</sup> See *id.* ("The FISA Court authorized an electronic surveillance of the computer and software within the Ames' residence. In addition, the Attorney General had authorized a warrantless physical search of the residence. At that time, FISA did not apply to physical searches.").

2007]

## DISAPPEARING SAFEGUARDS

189

Division on the case.<sup>102</sup> The DOJ had become “sloppy”<sup>103</sup> about complying with the primary purpose test, and Scruggs complained to Attorney General Janet Reno about the lack of information sharing controls.<sup>104</sup> The fear was that too much information sharing had taken place and that a defense motion to suppress the FISA evidence would be granted.<sup>105</sup> Under FISA, “criminal activity cannot be the primary purpose of the surveillance”<sup>106</sup> and a breach of this requirement would make any corresponding evidence inadmissible.<sup>107</sup>

Fortunately for the FBI, Ames pleaded guilty before his trial, without challenging the surveillance, so the potential violation of the primary purpose test was never addressed. After Ames pleaded guilty, FBI headquarters tightened its grip on information sharing, with a new rule that there were to be “no further contacts with prosecutors in [foreign counterintelligence] investigations without the permission of the OIPR, due to issues raised about [FISA] certifications.”<sup>108</sup> Furthermore, the Deputy Director of the FBI made it clear that any infraction of this rule would be a “career stopper.”<sup>109</sup>

In 1995, responding to concerns within the DOJ and the FBI about the use of FISA evidence in criminal prosecutions, and responding to the potential FISA violations that almost came to frui-

---

<sup>102</sup> BELLOWS REPORT, *supra* note 76, at 713 (Chapter 20, entitled “‘Primary Purpose’ and the Sharing of Intelligence Information Among the FBI, OIPR, and the Criminal Division,” details Scruggs’ belief that “the relationship that existed between the FBI and [Internal Security Section] during the Ames investigation could be used by defense counsel to cast doubt upon the ‘primary purpose’ of the FISA surveillance and thereby jeopardize the prosecution.”).

<sup>103</sup> *Id.* at 712.

<sup>104</sup> *Id.* at 713 (“Scruggs was concerned that there were no written guidelines governing contacts between the Criminal Division and the FBI. This coincided with issues arising from the investigation of Aldrich Ames.” (internal citations omitted)).

<sup>105</sup> *Id.* (“Scruggs raised concerns with the Attorney General that the FISA statute had been violated by these contacts [that the FBI had been having with prosecutors] and that her certifications had been inaccurate.”).

<sup>106</sup> *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (citations omitted).

<sup>107</sup> *See* Original FISA 1978, Pub. L. No. 95-511, § 106(e), 92 Stat. 1783, 1794 (1978) (codified as amended at 50 U.S.C. § 1806(e) (1994)) (“Any person against whom evidence obtained or derived from an electronic surveillance . . . may move to suppress the evidence . . . [if] (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval.”).

<sup>108</sup> BELLOWS REPORT, *supra* note 76, at 713 (Chapter 20, entitled “‘Primary Purpose’ and the Sharing of Intelligence Information Among the FBI, OIPR, and the Criminal Division”).

<sup>109</sup> *Id.* at 714.

R

R

tion in the Aldrich Ames investigation, Attorney General Janet Reno issued a memorandum (1995 Procedures) outlining guidelines for the interactions between investigative agents and prosecutors.<sup>110</sup> The purpose of the memo was to “avoid prejudicing a potential criminal prosecution” and to “avoid running afoul of the ‘primary purpose’ test.”<sup>111</sup> However, the 1995 Procedures only aggravated the situation and were “almost immediately misunderstood and misapplied.”<sup>112</sup> Vice Chairman of the Intelligence Committee, Richard C. Shelby, commented in a report from December 2002, that “[i]n short order, the OIPR attorneys turned the ‘primary purpose test’ into a *de facto* ‘exclusive purpose’ test.”<sup>113</sup> The result was a largely institutionally created barrier to information sharing, and the 1995 procedures came to be known as the “wall.”<sup>114</sup>

### C. Amendments to FISA

#### 1. *The Patriot Act*

Barriers to the flow of information between intelligence and law enforcement officials were widely cited as a significant cause of the intelligence failures which led to 9/11.<sup>115</sup> On October 26, 2001,

<sup>110</sup> Memorandum from Janet Reno, Attorney Gen., to Assistant Attorney Gen., Criminal Div., et al. (July 19, 1995), available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html> [hereinafter 1995 Procedures].

<sup>111</sup> BELLOWS REPORT, *supra* note 76, at 721 (Chapter 20, entitled “‘Primary Purpose’ and the Sharing of Intelligence Information Among the FBI, OIPR, and the Criminal Division”).

<sup>112</sup> THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 79 (2004) [hereinafter 911 COMMISSION REPORT].

<sup>113</sup> SHELBY REPORT, *supra* note 95, at 49 (quoting GAO REPORT, *supra* note 78, at 14).

<sup>114</sup> 911 COMMISSION REPORT, *supra* note 112, at 79; GAO REPORT, *supra* note 78, at 4 (documenting that “[t]he implementation and interpretation of the [Attorney General’s 1995] procedures . . . led to a significant decline in coordination between the FBI and the Criminal Division”). The FISC also pressured against information sharing, in as much as it “was aware that the [Attorney General’s 1995] procedures were being followed by the Department [of Justice] and apparently adopted elements of them in certain cases.” *In re Sealed Case*, 310 F.3d 717, 728 (FISA Ct. Rev. 2002).

<sup>115</sup> See, e.g., SHELBY REPORT, *supra* note 95, at 4–5 (referring to information sharing barriers as “profound flaws”).

Our Joint Inquiry has highlighted fundamental problems with information-sharing within the IC [Intelligence Community], depriving analysts of the information access they need in order to draw the inferences and develop the conclusions necessary to inform decision-making. The IC’s abject failure to ‘connect the dots’ before September 11, 2001 illustrates the need to wholly rethink the Community’s approach to these issues. The CIA’s chronic failure,

R

R

R

R

following only a few weeks of debate and limited hearings, the final version of the 352-page Patriot Act became law.<sup>116</sup> The Act amended FISA in several areas and two provisions effectively dismantled the wall which had restricted information flow within the government.<sup>117</sup>

The “significant purpose” amendment, section 218 of the Patriot Act, was designed to facilitate greater coordination between intelligence and law enforcement officials and to overturn prior standards restricting that coordination.<sup>118</sup> The new language required certification that “a significant purpose”—rather than “the purpose”—of any FISA surveillance would be to collect foreign intelligence information. The consequence of the amendment was that FISA surveillance could now be authorized primarily for criminal purposes, so long as a significant purpose for collecting foreign intelligence information remained. The amendment eliminated the primary purpose test,<sup>119</sup> and “ma[de] it easier for law enforcement to obtain a FISA search or surveillance warrant . . . .”<sup>120</sup>

Senators Leahy and Feingold both expressed apprehension over relaxing the FISA “purpose” language. Senator Leahy described the change as “very problematic.”<sup>121</sup> He said that it would now be “easier for the FBI to use a FISA wiretap to obtain information where the Government’s most important motivation for the wiretap is for use in a criminal prosecution.”<sup>122</sup> Senator Feingold forecasted that the government would obtain FISA approvals, the primary purpose of which was a criminal investigation, and that this change would raise Fourth Amendment concerns.<sup>123</sup>

---

before September 11, to share with other agencies the names of known Al-Qa’ida terrorists who it knew to be in the country allowed at least two such terrorists the opportunity to live, move, and prepare for the attacks without hindrance from the very federal officials whose job it is to find them.

*Id.*

<sup>116</sup> Patriot Act, Pub. L. No. 107-56, §§ 206–208, 214, 215, 218, 504, 1003, 115 Stat. 272 (2001) (codified as amended at 50 U.S.C. §§ 1805(c)(2)(B), 1805(e)(1), 1824(d), 1803(a), 1805(f), 1842, 1843, 1861, 1862, 1804(a)(7)(B), 1806(k), 1825(k), 1801(f)(2) (2001) (Senator Feingold cast the only dissenting vote).

<sup>117</sup> Patriot Act § 218 (codified as 50 U.S.C. §§ 1804(a)(7)(B), 504).

<sup>118</sup> *Id.*

<sup>119</sup> See, e.g., *In re Sealed Case*, 310 F.3d at 734 (“[T]he Patriot Act amendments clearly disapprove the primary purpose test.”).

<sup>120</sup> *Id.* at 733.

<sup>121</sup> 147 CONG. REC. S10593 (2001) (statement of Sen. Leahy), quoted in *In re Sealed Case*, 310 F.3d at 733.

<sup>122</sup> *Id.*

<sup>123</sup> *Id.*

In addition to dismantling the wall, the Patriot Act made several other substantial changes to FISA. Section 206 of the Patriot Act amended FISA to enable issuance of “roving wiretaps”—warrants that would follow a target, not the phone.<sup>124</sup> This section was enacted to defeat tactics used by counterintelligence targets for evading electronic surveillance, such as rapidly changing cell phones, internet accounts, or meeting venues.<sup>125</sup> Roving wiretaps allow the government to intercept communications without specifying the particular telephone line, computer or other facility to be monitored. Critics point out that criminal roving wiretap laws require that the eavesdropper make sure the target is actually using the device being monitored, a safeguard not employed by FISA.<sup>126</sup>

Section 207 of the Patriot Act increased the duration of FISA surveillance on agents of a foreign power from ninety to 120 days.<sup>127</sup> It also expanded the duration of physical search orders from forty-five to ninety days<sup>128</sup> and increased the FISC from seven to eleven judges, three of whom must reside in Washington, D.C.<sup>129</sup> The government was also given up to seventy-two hours to wiretap a suspect before a court order was made.<sup>130</sup>

Pen Register/Trap and Trace authority, under FISA, was amended by section 214 of the Patriot Act.<sup>131</sup> Pen registers are surveillance devices that capture the phone numbers dialed on outgoing telephone calls; trap and trace devices capture the numbers

---

<sup>124</sup> See Patriot Act, Pub. L. No. 107-56, § 206, *115 Stat. 272, 282 (2001)* (codified at 50 U.S.C. § 1805(c)(2)(B) (2001)).

<sup>125</sup> Patriot Act § 206 (codified at 50 U.S.C. § 1805(c)(2)(B) (2001)).

<sup>126</sup> See Memorandum from Office of the Gen. Counsel, drafted by Michael Woods, to FBI, all Divs. 3–4 (Oct. 26, 2001), *available at* <http://www.fas.org/irp/agency/doj/fisa/doj-fisa-patriot-122302c.pdf>, *attached to* letter from Daniel J. Bryant, Assistant Attorney Gen. to Hon. Russell D. Feingold, Chairman, Subcomm. on the Constitution Comm. on the Judiciary (Dec. 23, 2002) (on file with author) [hereinafter FBI Woods Memo].

Proposals have been made which would require more stringent rules on roving wiretaps. For example, H.R. 1526, 108th Cong. (2004) (introduced by Rep. Otter) and S. Res. 737, 108th Cong. (2004) (introduced by Sen. Craig) (the SAFE Acts) would “require in the case of FISA roving wiretaps that either identity of the target or the nature and location of the targeted facilities be specified, that if the nature and location are not known surveillance be limited to times when the target is present.” CHARLES DOYLE, AM. LAW DIV., CONG. RESEARCH SERV., USA PATRIOT ACT REAUTHORIZATION PROPOSALS AND RELATED MATTERS IN BRIEF 5, <http://www.fas.org/sgp/crs/intel/RS22196.pdf>.

<sup>127</sup> Patriot Act § 207 (codified at 50 U.S.C. § 1805(e)(1) (2001)).

<sup>128</sup> Patriot Act § 207 (codified at 50 U.S.C. § 1824(d) (2001)).

<sup>129</sup> Patriot Act § 207 (codified at 50 U.S.C. § 1803(a) (2001)).

<sup>130</sup> Patriot Act § 207 (codified at 50 U.S.C. § 1805(f) (2001)).

<sup>131</sup> Patriot Act § 214 (codified at 50 U.S.C. §§ 1842, 1843 (2001)).

identifying incoming calls. The former “specific and articulable facts” standard, which was required for FISA applications seeking telephone “trap and trace” information, was reduced to a simple “relevance” standard, prompting criticism that the relaxed standard was too low.<sup>132</sup>

Another controversial Patriot Act provision, section 215, changed FISA to allow the FBI to seize “any tangible thing,” including highly sensitive medical, library, business, and travel records from a wide variety of institutions.<sup>133</sup> Critics of section 215 point out that for these seizures the government does not need to show that the target is an agent of a foreign power. Also, the “any tangible thing” warrant *must* be granted by the court if the application satisfies the requirements,<sup>134</sup> and strict gag orders are placed on persons served with the request.<sup>135</sup> Although the Department of Justice must provide Congress with a semiannual report on the number of applications made and the number granted or denied, there is no required reporting to the court or Congress regarding actual documents seized or their usefulness.<sup>136</sup>

Congress also added Patriot Act section 504, which is not subject to sunset, to require intelligence and law enforcement operatives to “coordinate efforts to investigate or protect against” national security threats.<sup>137</sup>

a. FISC Decision: May 17, 2002

The events surrounding the FISC decision of May 17, 2002 amounted to a showdown over the implementation of the Patriot Act amendments into FISA—the FISC-opposed implementation, and the Attorney General-endorsed implementation. In a rare<sup>138</sup>

---

<sup>132</sup> See FBI Woods Memo, *supra* note 126, at 4.

<sup>133</sup> Patriot Act § 215 (codified at 50 U.S.C. §§ 1861, 1862 (2001)). See also FBI Woods Memo, *supra* note 126, at 4.

<sup>134</sup> Patriot Act § 215 (codified at 50 U.S.C. § 1861(c)(1) (2001)).

<sup>135</sup> Patriot Act § 215 (codified at 50 U.S.C. § 1861(d)(2001) (“No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section) . . .”).

<sup>136</sup> Patriot Act § 215 (codified at 50 U.S.C. § 1862 (2001)).

<sup>137</sup> Patriot Act § 504 (codified at 50 U.S.C. §§ 1806(k), 1825(k) (2001)).

<sup>138</sup> The FISC decision was made public in August of 2002, making it only the second opinion ever published by the FISC. The FISC had released a brief opinion in 1981 explaining the court’s lack of jurisdiction over physical searches. FISA was originally enacted only to allow electronic wiretapping, but was later amended by Congress in 1994 to allow physical searches. See 50 U.S.C. §§ 1821–1829 (2006).

en banc decision,<sup>139</sup> the FISC rejected the Patriot Act amendments.<sup>140</sup> The decision was officially worded as an *approval* of the government's FISA application, rather than a *denial* of a motion to implement the Patriot Act amendments, which allowed the FISC to foreclose any appeal to the FISCRC and entrench its opposition to the Patriot Act.<sup>141</sup>

Apparently anticipating this showdown, in November 2001 (after the Patriot Act was passed but before its May 17, 2002 decision), the FISC formally adopted Attorney General Janet Reno's amended 1995 procedures, calling them "minimization procedures" to be followed by all subsequent FISA cases.<sup>142</sup> (In order to safeguard privacy rights, FISA has always required that procedures be followed by the Attorney General to "minimize the acquisition and retention, and prohibit the dissemination" of information gathered on United States persons. Intelligence that is gathered under FISA may not be disclosed or disseminated, except as allowed by the

---

Interestingly, the May 17 FISC decision was only obtained after Senators Leahy, Grassley and Specter submitted a direct request to the presiding FISC judge that the court "[p]lease provide, or authorize the Justice Department to provide, copies of those [2002] procedures as submitted and as revised, any memorandum opinion(s) of the Court that explain the rationale for those revisions, and any legal memoranda submitted on this matter by the Department of Justice." Letter from Senators Patrick Leahy, Charles E. Grassley, and Arlen Specter, members of the Senate Select Comm. on Intelligence, to Colleen Kollar-Kotelly, Presiding Judge, Foreign Intelligence Surveillance Court (July 30, 2002), <http://www.fas.org/irp/agency/doj/fisa/leahy073102.html>. See FISC decision, 218 F. Supp. 2d 611, 613 (FISA Ct. 2002).

<sup>139</sup> See Lerner, *supra* note 66, at 507 n.87.

The decision to hear the case *en banc* was plainly outside the statutory authority of the FISC. The FISA required each FISA application to be considered by a single judge. There was no mechanism for appeal to an en banc court; the FISA makes clear that the only relief permitted is an appeal to the Foreign Intelligence Surveillance Court of Review.

*Id.* (citing 50 U.S.C. §§ 1803(a), 1822(c)).

<sup>140</sup> See FISC decision, 218 F. Supp. 2d at 613.

<sup>141</sup> The May 17 FISC decision officially granted the government's motion, with the exception that the procedures be modified in part. See *id.* Appeals to the FISCRC may only be made when the FISC has *denied* an application for FISA warrant. 50 U.S.C. § 1803(b) (2006) (FISA grants the FISCRC "jurisdiction to review the denial of any application.").

<sup>142</sup> See *In re Sealed Case*, 310 F.3d 717, 729 (FISA Ct. Rev. 2002).

Although the Patriot Act amendments to FISA expressly sanctioned consultation and coordination between intelligence and law enforcement officials, in response to the first [FISA] applications filed by OIPR under those amendments, in November 2001, the FISA court for the first time adopted the 1995 Procedures, as augmented by the January 2000 and August 2001 Procedures, as "minimization procedures" to apply in all cases before the court.

*Id.*

minimization procedures.).<sup>143</sup> These 1995 procedures, as discussed *supra* Part II.B.3, prohibited information sharing and conflicted with the Patriot Act.<sup>144</sup>

In early 2002 Attorney General Ashcroft adopted a revised set of departmental procedures (2002 Procedures), which allowed and encouraged information sharing.<sup>145</sup> These 2002 Procedures set the Patriot Act amendments into motion. The Attorney General confronted the FISC by making a motion that the FISC vacate all lingering wall requirements that conflicted with the 2002 procedures.<sup>146</sup> The Attorney General sought approval that FISA, as amended by the Patriot Act, would support warrants issued “primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains.”<sup>147</sup>

The FISC struck down two important paragraphs in the 2002 Procedures which would have authorized federal prosecutors to advise FBI agents on FISA surveillance. The FISC revised the two paragraphs by inserting strong language derived from the 1995 Procedures that prohibited law enforcement officials from “direct[ing] or control[ling]” FISA investigations.<sup>148</sup> In addition, the FISC also imposed continued adherence to the “chaperone” requirement, which required the Office of Intelligence and Policy Review to be present during meetings involving intelligence and law enforcement coordination.<sup>149</sup>

---

<sup>143</sup> 50 U.S.C. § 1806(a) (2006).

<sup>144</sup> See *In re Sealed Case*, 310 F.3d at 727 (“Apparently to avoid running afoul of the primary purpose test used by some courts, the 1995 Procedures limited contacts between the FBI and the Criminal Division in cases where FISA surveillance or searches were being conducted by the FBI for foreign intelligence (FI) or foreign counterintelligence (FCI) purposes.”).

<sup>145</sup> Memorandum from John Ashcroft, Attorney Gen. to Dir., FBI, et al. 2 (Mar. 6, 2002), <http://www.fas.org/irp/agency/doj/fisa/ag030602.html> [hereinafter 2002 Procedures].

<sup>146</sup> *In re Sealed Case*, 310 F.3d at 729 (“The government also asked the FISA court to vacate its orders adopting the prior procedures as minimization procedures in all cases and imposing special ‘wall’ procedures in certain cases.”).

<sup>147</sup> FISC decision, 218 F. Supp. 2d 611, 615 n.2 (FISA Ct. 2002) (quoting the 2002 Procedures, *supra* note 145).

<sup>148</sup> *Id.* at 625. The FISC explained the dangerous implications of allowing law enforcement officials to advise FBI agents on FISA matters without oversight. “[C]riminal prosecutors will tell the FBI when to use FISA (perhaps because they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute.” *Id.* at 624.

<sup>149</sup> See *id.* at 625. The FISC stated that counterintelligence and criminal officers “may consult each other to coordinate their efforts” but the “OIPR shall be invited to all such consultations, and if they are unable to attend, OIPR shall be apprised of the substance of

The FISC thus prevented implementation of the Patriot Act amendments, and preserved the wall and the primary purpose test. The FISC rested its decision on adherence to the 1995 Procedures (calling them “minimization procedures”),<sup>150</sup> which disallowed information sharing.<sup>151</sup> Since the FISC rested its decision on these minimization procedures, it declined to reach the key issue of the Patriot Act’s impact on FISA. In fact, “one reading of the FISC decision is that the court attempted to duck the effects of the Patriot Act amendments.”<sup>152</sup> The FISC’s failure to reference the Patriot Act amendments left the court open for criticism, and, when the FISC eventually gained jurisdiction, ultimately reversal on appeal.

b. FISC Decision: Nov. 18, 2002

FISA grants the FISC “jurisdiction to review the *denial* of any application.”<sup>153</sup> The May 17, 2002 FISC decision *granted* the Attorney General’s FISA application.<sup>154</sup> Thus the government was unable to appeal the FISC decision directly. However, to create an avenue for appeal, the government applied for a FISA warrant on July 19, 2002 and “expressly proposed using the 2002 Procedures *without modification*.”<sup>155</sup> The FISC once again granted the FISA warrant, but amended the 2002 procedures to be consistent with the May 17 decision.<sup>156</sup> The government then appealed on the

---

the consultations forthwith in writing so that the Court may be notified at the earliest opportunity.” *Id.*

<sup>150</sup> *See id.* (stating that “[t]he purpose of minimization procedures . . . [is to] protect the privacy of Americans in these highly intrusive surveillances and searches” and that modifications to the Attorney General’s motion were necessary in order to “bring the [government’s proposed] minimization procedures into accord with the language used in the FISA.”). The FISC also stated its intention to “reinstate the bright line used in the 1995 procedures, on which the Court has relied.” *Id.*

<sup>151</sup> The FISC decision may have been influenced in part by events outside of the Patriot Act. For example, the FISC referred to a “troubling number of inaccurate FBI affidavits” and erroneous statements used in securing FISA warrants. *Id.* at 620. In 2000, for example, seventy-five errors were disclosed to the FISC by the FBI. *Id.* The FISC noted that “[i]n virtually every instance, the government’s misstatements and [errors] . . . involved information sharing and unauthorized disseminations.” *Id.* As a consequence, the FISC felt the need to take a “supervisory” role and took steps to “assess compliance with the ‘wall’ procedures.” *Id.*

<sup>152</sup> Banks, *supra* note 30, at 1170.

<sup>153</sup> 50 U.S.C. § 1803(b) (2006) (emphasis added).

<sup>154</sup> *See FISC decision*, 218 F. Supp. 2d at 613.

<sup>155</sup> *In re Sealed Case*, 310 F.3d 717, 730 (FISA Ct. Rev. 2002) (emphasis in original).

<sup>156</sup> *Id.* Three months later, on October 19, 2002, the government applied for a renewal of the modified July 19 application, and again proposed to use the 2002 procedures without

grounds that the FISC had partially denied the application and the FISCR took jurisdiction.<sup>157</sup>

On appeal to the FISCR, the government argued that the primary purpose test did not exist in the original FISA, but instead was invented by lower federal courts.<sup>158</sup> The government argued that, even if the primary purpose test did exist, it was obviated by the Patriot Act.<sup>159</sup> The government also argued that FISA, as amended by the Patriot Act, did not violate the Fourth Amendment because the Fourth Amendment did not compel the primary purpose test.<sup>160</sup>

The FISCR agreed with the government that the primary purpose test was a misreading of the original FISA, and that what existed was a “false dichotomy” between intelligence and law enforcement.<sup>161</sup> The FISCR found it “quite puzzling”<sup>162</sup> that the Department of Justice and several federal courts would read into the original FISA a primary purpose requirement, especially when an “obvious reading of the statutory language” showed that “foreign intelligence information includes evidence of foreign intelligence crimes.”<sup>163</sup> The legislative history shows that in enacting FISA, Congress did anticipate an overlap between foreign intelli-

---

modification. Again the FISC granted the application, but amended the procedures. The jurisdiction obtained by the FISCR relied on the partial denial of both the July 19 and October 17 applications.

<sup>157</sup> *See id.* at 721. The FISCR reasoned:

The FISA court’s order is styled as a grant of the application “as modified.” It seems obvious, however, that the FISA court’s order actually denied the application to the extent it rejected a significant portion of the government’s proposed minimization procedures and imposed restrictions on Department of Justice investigations that the government opposes. Indeed, the FISA court was clear in rejecting a portion of the application. Under these circumstances, we have jurisdiction to review the FISA court’s order; to conclude otherwise would elevate form over substance and deprive the government of judicial review of the minimization procedures imposed by the FISA court.

*Id.*

<sup>158</sup> *See id.* at 726 (“Several circuits have followed *Truong* in applying similar versions of the ‘primary purpose’ test, despite the fact that *Truong* was not a FISA decision.”).

<sup>159</sup> Supp. Brief for United States, *supra* note 30, at Part II(C) (“[T]he USA Patriot Act . . . eliminates the ‘primary purpose’ standard.”).

<sup>160</sup> *See In re Sealed Case*, 310 F.3d at 736 (“FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is *not* criminal prosecution.”).

<sup>161</sup> *Id.* at 735. The FISCR stated further that the primary purpose test originated with *Truong*, a federal district court, not a FISA court. *Id.* at 742.

<sup>162</sup> *Id.* at 723.

<sup>163</sup> *Id.*

gence gathering and criminal prosecution.<sup>164</sup> The FISCR also noted that “arresting and prosecuting terrorist agents . . . may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity.”<sup>165</sup>

The FISCR described the “significant purpose” amendment as an “analytic conundrum”<sup>166</sup> that “muddied the landscape,”<sup>167</sup> but noted that the issue was “moot” in light of its opinion<sup>168</sup> because even though “the original FISA did not contemplate the ‘false dichotomy,’ the Patriot Act actually did—which makes it no longer false.”<sup>169</sup> In other words, whether the wall was imposed by the original FISA statute, or whether it was created improperly through court decisions or department practice was irrelevant because, in any event, the Patriot Act had expressly removed it.<sup>170</sup>

---

<sup>164</sup> See, e.g., SEN. REP. 95-701, at 11 (1978) (“[Foreign intelligence] surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area.”).

Obviously, use of “foreign intelligence information” as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving [these activities] can be sought, retained, and used pursuant to this bill.

H.R. REP. NO. 95-1283, at 49 (1978). But see H.R. REP. NO. 95-1283, at 36 (“[S]urveillance under this bill are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information.”). The FISCR debunked the legislative history that supported the primary purpose test, calling the comments “an observation, not a prescription.” *In re Sealed Case*, 310 F.3d at 725.

<sup>165</sup> *In re Sealed Case*, 310 F.3d at 724.

<sup>166</sup> *Id.* at 735.

<sup>167</sup> *Id.* at 728.

<sup>168</sup> *Id.* at 729 n.18.

<sup>169</sup> *Id.* at 735.

<sup>170</sup> *Id.* at 733 (“Indeed, [Congress] went further to emphasize its purpose in breaking down barriers between criminal law enforcement and intelligence (or counterintelligence) gathering by adding [FISA] section 1806(k) [which authorizes consultation and coordination between the FBI and federal prosecutors].”). See also *id.* at 735 (“The important point is—and here we agree with the government—the Patriot Act amendment, by using the word “significant,” eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses.”).

It is also interesting to note that the government’s argument that the wall never existed was made exclusively on appeal, despite the fact that arguments in federal appeals courts cannot originate at the appellate level. Judge Silberman actually outlined the argument for Solicitor General Olson during the hearing, which the government then wrote-up and submitted in a supplemental brief. See Banks, *supra* note 30, at 1174. See also *In re Sealed Case*, 310 F.3d at 721; Transcript of Hearing at 5, *In re Sealed Case*, 310 F.3d at 721 (Sept. 9, 2002) (No. 02-001), available at <http://www.fas.org/irp/agency/doj/fisa/>

The FISCER also agreed with the government that the “significant purpose” amendment did not violate the Fourth Amendment. In balancing the government’s need to protect national security and the citizen’s right to individual privacy, the FISCER said that “the threat to society is . . . a crucial factor” and “[o]ur case may well involve the most serious threat our country faces.”<sup>171</sup> The FISCER concluded that “applying the balancing test” that “FISA as amended is constitutional because the surveillances it authorizes are reasonable.”<sup>172</sup>

The FISCER overturned the en banc FISC decision, approving the “significant purpose” provision, and approving the Attorney General’s 2002 procedures. However, the FISCER has been criticized as “[u]nschooled in FISA and its implementation.”<sup>173</sup> It is true that when the FISCER rendered its 2002 decision, the three presiding FISCER judges had never before heard a FISA case, whereas the veteran lower FISC court had been conducting FISA hearings for over twenty years.<sup>174</sup> The primary purpose commentary made by the FISCER, in particular, was sharply criticized. “It is hardly credible that the [FISCER] judges would be puzzled by a practice that had been supported as a bedrock component of FISA by dozens of FISC judges and by Congress for twenty-four years.”<sup>175</sup>

---

hrng090902.htm. Judge Silberman explained: “Since proceedings before the FISA court and the Court of Review are *ex parte*—not adversarial—we can entertain an argument supporting the government’s position not presented to the lower court.” *In re Sealed Case*, 310 F.3d at 721 n.6.

Interestingly, the FISCER decision was not Judge Silberman’s first substantial encounter with FISA. Judge Silberman had been embroiled in FISA debate in the mid-1970s, before FISA was enacted. The judge, a former Deputy Attorney General, testified in strong opposition to FISA before the Subcommittee on Legislation. In those hearings in 1978, Mr. Silberman declared that FISA was “an enormous and fundamental mistake which the Congress and the American people would have reason to regret.” *Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Legislation of the House Permanent Select Comm. on Intelligence*, 95th Cong., 2d Sess. 217 (1978) (statement of Laurence Silberman), <http://www.cnss.org/fisa011078.pdf>.

<sup>171</sup> *In re Sealed Case*, 310 F.3d at 746.

<sup>172</sup> *Id.*

<sup>173</sup> Banks, *supra* note 30, at 1174.

<sup>174</sup> *In re Sealed Case*, 310 F.3d at 719 (“This is the first appeal from the Foreign Intelligence Surveillance Court to the Court of Review since the passage of the Foreign Intelligence Surveillance Act.”).

<sup>175</sup> Banks, *supra* note 30, at 1175.

R

R

## 2. The "Lone Wolf" Amendment

In December 2004 Congress amended FISA by expanding the definition of "agent of a foreign power."<sup>176</sup> The so-called "Lone Wolf" Amendment was passed to give the government more power to fight new threats posed by non-United States persons<sup>177</sup> acting independent of foreign direction.<sup>178</sup> When FISA was originally passed, terrorists typically formed around an organized group, but today, since individuals or radicals often act alone, the government sought to have the law updated to reflect the changing conditions.<sup>179</sup>

The Lone Wolf Amendment was enacted in the wake of the high profile controversy involving Zacarias Moussaoui, a suspected terrorist whose unsearched computer files contained clues to the 9/11 plot.<sup>180</sup> Moussaoui was arrested in Minnesota in August of 2001.<sup>181</sup> The FBI never applied for a FISA warrant to search his

---

<sup>176</sup> See Lone Wolf Amendment, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004) (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2004)), which does not require the government to prove a nexus with a foreign power. The Lone Wolf Amendment only applies to nonresident aliens. See *infra* note 177.

<sup>177</sup> § 1801(b)(1)(C) (defining "agent of a foreign power" as "any person *other than a United States person*, who . . . engages in international terrorism or activities in preparation therefore [sic]") (emphasis added).

<sup>178</sup> S. REP. NO. 108-40, at 1 (2003). The report stated: "In light of the significant risk of devastating attacks that can be carried out by non-United States persons acting alone, individual terrorists must be monitored and stopped, regardless of whether they operate in coordination with other individuals or organizations." *Id.*

<sup>179</sup> See S. REP. NO. 108-40, at 4 (2003) (quoting Spike Bowman, the Deputy General Counsel of the FBI). Mr. Bowman stated:

When FISA was enacted, terrorism was very different from what we see today. . . . Where we once saw terrorism formed solely around organized groups, today we often see individuals willing to commit indiscriminate acts of terror. It may be that these individuals are affiliated with groups we do not see, but it may be that they are simply radicals who desire to bring about destruction.

*Id.*

<sup>180</sup> See Romesh Ratnesar & Michael Weisskopf, *How the FBI Blew the Case: The Inside Story of the FBI Whistle-Blower Who Accuses Her Bosses of Ignoring Warnings of 9/11. A Reading of Her Entire Memo Suggests a Bracing Blueprint for Change*, TIME, May 27, 2002, <http://archives.cnn.com/2002/ALLPOLITICS/05/27/time.fbi/> (quoting FBI agent Coleen Rowly stating that "[t]here is at least some chance that [a FISA warrant to search Moussaoui's computer] . . . may have limited the Sept. 11th attacks and resulting loss of life."). When investigators, under a Title III search warrant, eventually searched the laptop after 9/11 they found evidence of the terrorist plot that could have prevented the attacks. *Id.*

<sup>181</sup> See generally Patrick Martin, *The Strange Case of Zacarias Moussaoui*, WORLD SOCIALIST WEB SITE, Jan. 5, 2002, <http://www.wsws.org/articles/2002/jan2002/mous-j05.shtml>.

Moussaoui was arrested in Minnesota August 16 after officials of a flight school, the Pan Am International Flight Academy in Eagan, a suburb of Minneapolis, tipped off the FBI that he was seeking flight training on a Boeing 747

home or personal effects, “precisely because [FBI Headquarters] concluded that there was insufficient evidence (amounting to probable cause) connecting Moussaoui to a foreign power.”<sup>182</sup> The government hoped the Lone Wolf Amendment would be a “Moussaoui fix.”<sup>183</sup>

The Lone Wolf Amendment only applies to nonresident aliens.<sup>184</sup> However, as will be discussed in Part III, the fruits of nonresident alien wiretaps can be used against United States citizens, so the effects of relaxing the requirement against nonresident aliens can also be felt by United States citizens. Critics of the amendment argue that it “writes out . . . a key requirement necessary to the lawfulness of such searches.”<sup>185</sup>

### 3. USA PATRIOT Improvement and Reauthorization Act of 2005

On March 9, 2006, one day before the Patriot Act sunset provisions were scheduled to become effective,<sup>186</sup> Congress enacted legislation to expand FISA surveillance authority over nonresident

---

jumbo jet. His conduct aroused suspicion: his attitude was belligerent, he was evasive about his personal background, he declined to speak French with an instructor who knew the language, and he paid the \$6,300 fee in cash. He insisted on training to fly a jumbo jet despite an obvious lack of skill even with small planes. The prospective student reportedly did not want to learn how to take off or land, only how to steer the jet while it was in the air.

*Id.*

<sup>182</sup> Lerner, *supra* note 66, at 503. See also S. REP. NO. 108-40, at 3 (“One of the principal factors that prevented the issuance of such a warrant [on Moussaoui] was FISA’s requirement that the target be an agent of a foreign power.”).

**R**

<sup>183</sup> See, e.g., S. REP. NO. 108-40, at 11 (addressing the shortcomings of the Lone Wolf Amendment). Senators Leahy and Feingold suggest that “[w]ith catchy monikers like the ‘Moussaoui fix’ and the ‘lone wolf’ bill, it is aimed at making Americans feel safer, but it does not address the chronic problems that actually plague the effectiveness of our intelligence gatherers.” *Id.*

<sup>184</sup> See *supra* note 177. “United States person” is defined at 50 U.S.C. § 1801(i) (2006). The term “nonresident alien” includes people who are *not* United States persons. See *infra* notes 200–201 and accompanying text.

**R**

**R**

<sup>185</sup> S. REP. NO. 108-40, at 6 n.3 (quoting Senator Feingold).

<sup>186</sup> Patriot Act sunset provisions were initially scheduled to take effect on December 31, 2005, but were extended twice by Congress to push the date back to March 9, 2006. See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 105, 120 Stat 192, 195 (2006) (codified as amended at 50 U.S.C. §§ 1805, 1824(d) (2006)) [hereinafter Improvement and Reauthorization Act of 2005]; USA Patriot Act Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, §§ 3, 4, 120 Stat. 278, 278–281 (2006) (codified at 50 U.S.C. § 1861(f), 1861(d)(1), 1861(d)(2)(C)) [hereinafter Additional Reauthorizing Amendments Act of 2006].

aliens<sup>187</sup> and once again push back the FISA sunset provision deadlines to 2009.<sup>188</sup> Section 105 of the USA PATRIOT Improvement and Reauthorization Act of 2005 extended the maximum duration of FISA surveillance and physical search orders against nonresident aliens.<sup>189</sup> Initial orders authorizing such searches on nonresident aliens were extended to up to 120 days, and renewal orders were permitted to extend to up to one year.<sup>190</sup> Similarly, initial orders and extension orders authorizing installation and use of FISA pen registers and trap and trace devices were extended from a period of ninety days to one year in cases where the government could certify that the information likely to be obtained was foreign intelligence information not concerning a United States person.<sup>191</sup> In short, the USA PATRIOT Improvement and Reauthorization Act of 2005 again widened the disparity between United States persons and nonresident aliens.<sup>192</sup>

### III. THE NONRESIDENT ALIEN “LOOPHOLE” SHOULD BE REEXAMINED

Congress articulated that its goal in enacting FISA was finding the proper balance between an individual’s right to be free from unreasonable searches and seizures on the one hand, and the government’s interest in national security on the other.<sup>193</sup> With respect to the dichotomy between United States persons and nonresident aliens, Congress was fully aware that reducing safeguards against nonresident aliens would raise constitutional questions, including Fourth Amendment and equal protection issues.<sup>194</sup>

---

<sup>187</sup> See Improvement and Reauthorization Act of 2005 § 105 (codified as amended at 50 U.S.C. §§ 1805, 1824(d) (2006)).

<sup>188</sup> See Improvement and Reauthorization Act of 2005 § 103 (codified as amended at 50 U.S.C. §§ 1801 (2006)).

<sup>189</sup> See Improvement and Reauthorization Act of 2005 § 105 (codified as amended at 50 U.S.C. §§ 1805, 1824 (2006)) (authorizing surveillance duration increases on “any agent of a foreign power” “who is not a United States person”).

<sup>190</sup> *Id.*

<sup>191</sup> *Id.*

<sup>192</sup> The USA PATRIOT Improvement and Reauthorization Act of 2005 did seek to increase oversight into various FISA authority, but such safeguards were aimed only at United States persons. See Improvement and Reauthorization Act of 2005 §§ 106(a)(2), 106(b), 106(e), 106(f), 106(g), 106(h), 108(a)(1), 108(c), 109(a), 109(b), 109(d), 128(a), 128(b), 506 (codified as amended in various sections of 50 U.S.C. (2006)).

<sup>193</sup> See H.R. REP. NO. 95-1283 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf>.

<sup>194</sup> H.R. REP. NO. 95-1283, pt. 1, at 32–33 (acknowledging that “[s]ome have questioned whether it is constitutional to treat nonresident aliens differently from United States citi-

However, Congress ultimately concluded that “the protections afforded nonresident aliens in [FISA] fully satisfy the Constitution.”<sup>195</sup> Today, the few safeguards originally chosen by Congress and imposed on nonresident alien wiretapping have been slowly eroded by eight rounds of amendments passed in 1994, 1998, 1999, 2000, 2001, 2004, 2005, and 2006.<sup>196</sup> This section discusses the disappearing nonresident alien safeguards and their impact on United States persons.

---

zens, either because the nonresident aliens’ fourth amendment rights are violated or because to deny them protections afforded U.S. citizens denies them equal protection under the laws”).

<sup>195</sup> *Id.*

<sup>196</sup> Physical searches were added to FISA on October 14, 1994. *See* Counterintelligence and Security Enhancements Act of 1994, Pub. L. No. 103-359, tit. VIII, § 807(a)(1), (2), 108 Stat. 3423, 3443 (1994) (codified as amended at 50 U.S.C. §§ 1821–1829) [hereinafter Physical Searches Amendment 1994]. Pen register, trap and trace legislation was enacted on October 28, 1998. *See* Pen Register Amendment 1998, Pub. L. No. 105-272, tit. VI, §§ 601(1), 603(a), 112 Stat. 2404, 2412 (1998) (codified as amended at 50 U.S.C. §§ 1841–1846 (1998)). On December 3, 1999, the definition of “Agent of a foreign power” was expanded. *See* Agent of a Foreign Power Amendment 1999, Pub. L. No. 106-120, tit. VI, § 601, 113 Stat. 1606, 1619 (1999) (codified as amended at 50 U.S.C. § 1801(b)(2)(D)). Other various amendments were made on December 27, 2000. *See* Counterintelligence Reform Act of 2000, Pub. L. No. 106-567, title VI, § 601, 114 Stat. 2831, 2850 (codified as amended in various sections of 50 U.S.C.). Concerns about the wall were addressed on December 28, 2001. *See* Patriot Act, Pub. L. No. 107-56, §§ 206–208, 214, 215, 218, 504, 1003, 115 Stat. 272, 282, 283, 286, 291, 364, 392 (2001) (codified as amended at 50 U.S.C. §§ 1805(c)(2)(B), 1805(e)(1), 1824(d), 1803(a), 1805(f), 1842, 1843, 1861, 1862, 1804(a)(7)(B), 1806(k), 1825(k), 1801(f)(2) (2001)). Concerns about modernizing FISA to encompass terrorists acting with no nexus to any foreign power were addressed on December 17, 2004. *See* Lone Wolf Amendment, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004) (codified as amended at 50 U.S.C. § 1801(b)(1)(C)) (2004). In 2005 FISA’s sunset provisions were extended. *See* Extension of Sunset of Certain Provisions of the USA Patriot Act, Pub. L. No. 109-160, 119 Stat. 2957 (2005) (extending sunset provisions to February 3, 2006). In 2006 FISA’s sunset provisions were again extended. *See* Extension of Sunset of Certain Provisions of the USA Patriot Act, Pub. L. No. 109-170, 120 Stat. 3 (2006) (extending sunset provisions to March 10, 2006). Congress extended the sunset provisions again on March 9, 2006, and added substantive provisions to FISA which expanded the government’s ability to target nonresident aliens, but also added certain Congressional oversight over certain FISA authority with respect to United States persons. *See* Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 102, 105, 106(a)(2), 106(b), 106(e), 106(f), 106(g), 106(h), 108(a)(1), 108(c), 109(a), 109(b), 109(d), 128(a), 128(b), 506, 120 Stat 192, 194–205, 228, 229, 247 (2006) (codified in various sections of 50 U.S.C.). In 2006 Congress also added judicial review for the nondisclosure requirement of a FISA business record order, but only after a one-year waiting period has elapsed where the recipient may not challenge such an order. *See* Additional Reauthorizing Amendments Act of 2006, Pub. L. No. 109-178, §§ 3, 4, 120 Stat. 278, 278–281 (2006) (codified at 50 U.S.C. § 1861(f), 1861(d)(1), 1861(d)(2)(C)).

A. *Congress Purposefully Created a Dichotomy Between U.S. Persons and Nonresident Aliens*

Congress created two sets of standards that pervade FISA, one for United States persons and one for nonresident aliens.<sup>197</sup> Congress defined the first group, United States persons, to include “United States citizens and permanent resident aliens.”<sup>198</sup> Slyly, the second group, nonresident aliens, is never actually defined or even used in FISA.<sup>199</sup> Instead, the category of nonresident aliens is only known in the negative—i.e. *not* United States persons.<sup>200</sup> Thus, United States persons and nonresident aliens are mutually exclusive under FISA by definition—one group is defined as *not* the other.<sup>201</sup> To fully understand the dichotomy between the groups, every time one reads “United States person” one must also read “and *not* nonresident aliens.” Only when the term United States person is *not* used may one infer that a provision applies

<sup>197</sup> See, e.g., H.R. REP. NO. 95-1283, pt. 1, at 32 (stating that “the protections afforded [nonresident aliens] are not as great as those afforded United States persons.”).

<sup>198</sup> *Id.* The statutory definition of United States person actually also includes United States associations and corporations. See Original FISA 1978, Pub. L. No. 95-511, § 101(i), 92 Stat. 1783, 1786 (1978) (codified at 50 U.S.C. § 1801(i) (1978)—current version same as original). Original FISA 1978 defines a United States person as

a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 USCS § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

Original FISA 1978 § 101(i) (codified at 50 U.S.C. § 1801(i) (1978)—current version same as original).

<sup>199</sup> See 50 U.S.C. §§ 1801–1871 (never mentioning the words “nonresident alien(s)”).

<sup>200</sup> The Senate did elaborate in the legislative history that *not* United States persons—i.e. nonresident aliens—would include “illegal aliens, foreign terrorists, exchange visitors, foreign businessmen, foreign students, and foreign seamen.” S. REP. NO. 95-604, at 21 (1978). The House defined nonresident aliens almost identically as “aliens in the United States who are tourists, visiting businessmen, exchange visitors, foreign seamen, diplomatic and consular personnel, illegal aliens, etc.” H.R. REP. NO. 95-1283, pt. 1, at 32 (1978).

<sup>201</sup> See 50 U.S.C. § 1801(i) (definition of “United States person”). *Not* United States persons are casually referred to in the FISA legislative history as “nonresident aliens.” Even though the term “nonresident alien” is not found in FISA, the dichotomy drawn between the groups is clear. See, e.g., H.R. REP. NO. 95-1283, pt. 1, at 32–37 (discussing the constitutionality of reduced safeguards for nonresident aliens); INTERIM REPORT ON FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMM.: FISA IMPLEMENTATION FAILURES, 107TH CONG., § III(C)(4): The Working Relationship Between FBI Headquarters and Field Offices n. 23 (Feb. 25, 2003), [http://www.fas.org/irp/congress/2003\\_rpt/fisa.html](http://www.fas.org/irp/congress/2003_rpt/fisa.html) [hereinafter INTERIM REPORT: FBI IMPLEMENTATION FAILURES] (“[A] ‘non-U.S. person’ is, in effect, a non-resident alien.”).

across the board to both groups. Since the phrase “United States person” is used over sixty times in FISA, the examples of disparate treatment of the two groups is abundant.<sup>202</sup>

The rationale behind the alienage distinctions was, and still is, for the narrow purpose of protecting national security.<sup>203</sup> Congress observed that less intrusive techniques, i.e. those requiring additional safeguards, may be inadequate for collecting information on visitors who are only in the country for a short time.<sup>204</sup> In 1978, the Director of the FBI pointed out that “large numbers of temporary aliens visit the United States and that many of these aliens are working for foreign intelligence networks.”<sup>205</sup> In addition, the Select Committee on Intelligence Activities found that “one quarter of the Soviet exchange students coming to the United States in a

---

<sup>202</sup> Two prominent examples may be used to illustrate the dichotomy between “United States person” and its negative *not* United States person or “nonresident alien.” First, under the FISA minimization procedures FISA requires that “[i]nformation acquired from an electronic surveillance . . . concerning any *United States person* may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subtitle.” (emphasis added). 50 U.S.C. § 1806(a)(2006). Reading “United States person” to also mean “and *not* nonresident aliens,” the minimization procedures section, which strictly regulates dissemination of information obtained via FISA warrant, clearly applies *only* to United States persons and *not* to nonresident aliens. In other words, the language states that the government need *not* comply with minimization procedures when information collected pertains to nonresident aliens. Hence the minimization procedures safeguard applies only to United States persons.

Second, after the passage of the Lone Wolf Amendment in 2004, FISA relaxed the definition of an “agent of a foreign power” to include “any person *other than a United States person*, who . . . engages in international terrorism or activities in preparation therefore [sic].” (emphasis added). Before the amendment, the government was required to *always* link the target of the surveillance with a foreign power in order to receive approval for FISA surveillance. See Original FISA 1978 § 101(b) (codified at 50 U.S.C. § 1801(b) (1978) (“Agent of a foreign power”). After the amendment, if the target was a United States person, then the government would still be required to link the target to a foreign power. However, if the target was “any person other than a United States person,” i.e. a nonresident alien, then the government could obtain a FISA warrant without proving a nexus with a foreign power. In other words, the amendment was put in place to relax the restrictions on targeting terrorists acting outside of any foreign authority. Under the old FISA, the government could not obtain FISA warrants on such “lone wolves.”

<sup>203</sup> S. REP. NO. 95-604, at 21 (citing *Hampton v. Mow Sun Wong*, 426 U.S. 88 (1976)) (“[W]here there are compelling considerations of national security, alienage distinctions are clearly lawful.”).

<sup>204</sup> S. REP. NO. 95-604, at 21 (“[L]ess intrusive investigative techniques may not be able to obtain sufficient information about persons visiting here only for a limited time”) (emphasis removed).

<sup>205</sup> *Id.*

ten-year period were found to be intelligence officers.”<sup>206</sup> Congress found a reasonable probability that nonresident aliens would be engaging in activities that FISA was designed to protect.<sup>207</sup> Congress also found justification in the government’s need to be able to act swiftly against targets who are unlikely to remain permanently in the United States.<sup>208</sup> Thus, Congress has reduced the requirements for targeting nonresident aliens, but only after sufficient evidence was presented indicating the need for such a reduction, and only after carefully considering that the remaining safeguards—mainly the primary purpose requirement and the nexus with a foreign power requirement—were still intact with respect to nonresident aliens.

B. *United States v. Duggan and Circumventing  
the FISA Requirements*

Imagine that the government sought to target a feared group for search or surveillance under FISA, but that the government had insufficient evidence to obtain a FISA warrant. (For example, suppose the government was unable to demonstrate a nexus between the target and a foreign power; or that there was insufficient evidence to show probable cause that the target was involved or about to be involved in a criminal act; or that there was no emergency situation otherwise compelling issuance of a FISA warrant).<sup>209</sup> If one person in the feared group were a nonresident alien, or if someone close to or related to the feared group were a nonresident alien, then the government could bypass the FISA requirements by simply submitting a FISA application for the non-

---

<sup>206</sup> *Id.*

<sup>207</sup> See *United States v. Duggan*, 743 F.2d 59, 76 (2d Cir. 1984). The legislative history of FISA also supports bifurcating the system of safeguards. See S. REP. NO. 95-604, at 20. The Senate reasoned that “it is presumed that nonresident aliens who are officers or employees of a foreign power are likely sources of foreign intelligence information.” *Id.* Furthermore, the Senate concluded that

[g]iven the tenuous relationship of foreign officers or employees with the United States and their close relationship with a foreign power, this standard is considered by the Committee to be reasonable in light of the government’s legitimate need for foreign intelligence information and the nature of the interests upon which the search would intrude.

*Id.*

<sup>208</sup> *Id.* at 21.

<sup>209</sup> For a discussion of the basic FISA requirements, see *supra* Part II.B.

resident alien under the reduced (almost non-existent) standard.<sup>210</sup> The FISA warrant on the nonresident alien could include “bugs” in public places frequented by the nonresident alien, eavesdropping of telephone conversations, and searches of premises inhabited by or frequented by the nonresident alien.<sup>211</sup> It is not difficult to imagine that such broad surveillance instruments could serve to intercept a wide variety of United States persons’ activities that would otherwise be unapproved of or prohibited by FISA.<sup>212</sup> In short, the nonresident alien loophole is simply a work-around that the government can use when it cannot meet FISA standards; and the work-around allows the government to vicariously target United States persons against whom insufficient evidence exists to obtain a criminal warrant or a FISA warrant.<sup>213</sup> Additionally, the nonresident alien loophole enables the government to conduct “fishing expeditions” on less than probable cause, without a nexus with a foreign power, and without an emergency, just so long as the initial target is a nonresident alien.<sup>214</sup>

In *United States v. Duggan*,<sup>215</sup> the defendant Duggan, a United States citizen, faced a prosecution based on information obtained from a FISA warrant that targeted a nonresident alien, Megahey. Duggan and Megahey were members of the Provisional Irish Republican Army and were involved in acquiring explosives, weapons, ammunition, and remote-controlled detonation devices to be exported to Northern Ireland for use in terrorist activities.<sup>216</sup> Both defendants were living in the United States at the time. Megahey was an Irish national who sought political asylum in the United

---

<sup>210</sup> See *infra* Part III.C for the propositions (i) that none of the original safeguards exists for applications sought for nonresident aliens, and (ii) that, today, the application for a nonresident alien FISA warrant is barely more than a filing requirement.

<sup>211</sup> For a further examination of similar FISA surveillance hypotheticals, see 149 CONG. REC. S12387 (daily ed. Oct. 2, 2003) (statement of Sen. Craig), available at [http://www.fas.org/irp/congress/2003\\_cr/s1709.html](http://www.fas.org/irp/congress/2003_cr/s1709.html).

<sup>212</sup> *Id.*

<sup>213</sup> See *infra* notes 219–224 and accompanying text.

<sup>214</sup> See, e.g., *The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearings on S. 1448 Before the Select Comm. on Intelligence*, 107th Cong. 449 (2001) (statement of Jerry Berman, Executive Director, Center For Democracy and Technology) (stating that “judicial supervision is to ensure that there are not fishing expeditions,” and proposing that “since no FISA wiretap or extension except one has been turned down in the 22-year history of the statute, what is the bureaucratic problem of continuing that [judicial] supervision?”), available at [http://www.fas.org/irp/congress/2001\\_hr/ssci092401.html](http://www.fas.org/irp/congress/2001_hr/ssci092401.html).

<sup>215</sup> *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

<sup>216</sup> *Id.* at 65.

States, and Duggan, Megahey's assistant, was an American citizen.<sup>217</sup> They appealed a judgment of the United States District Court for the Eastern District of New York that convicted them of violations concerning the shipping of explosives and firearms.<sup>218</sup>

Duggan challenged his conviction on the basis that incriminating evidence against him violated the probable cause requirement of the Fourth Amendment.<sup>219</sup> Because Duggan was a United States citizen, preconditions to granting a FISA order on him would have been far more stringent than they were for the surveillance of Megahey, the nonresident alien.<sup>220</sup> Duggan argued that the government circumvented the heftier requirements for targeting a United States person by obtaining the warrant only against Megahey.

The court rejected Duggan's argument and said that "[i]t is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named"<sup>221</sup> and that "where there are compelling considerations of national security, alienage distinctions are clearly lawful."<sup>222</sup> The court held that a FISA warrant was properly obtained for the surveillance of Megahey and Duggan<sup>223</sup> and that surveillance ordered for national security purposes was properly used against the defendants in the criminal action.<sup>224</sup> Normally, FISA targets like Megahey never

---

<sup>217</sup> *Id.*

<sup>218</sup> *Id.* at 64.

<sup>219</sup> *Id.*

<sup>220</sup> *Id.* at 76.

<sup>221</sup> *Id.* at 80 (quoting *United States v. Donovan*, 429 U.S. 413, 416 (1977)). The court emphasized this point again later in the opinion stating that "otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial." *Id.* at 78.

<sup>222</sup> *Id.* at 76 (quoting S. REP. NO. 95-604, at 21 (1978)). In rejecting Duggan's constitutional arguments, the Court also noted that "[a]lthough both the Fourth Amendment and the Equal Protection Clause afford protection to all aliens, nothing in either provision prevents Congress from adopting standards and procedures that are more beneficial to United States citizens and resident aliens than to nonresident aliens, so long as the differences are reasonable." (citations omitted). *Id.* at 75.

<sup>223</sup> *Id.* at 79 (upholding denial of motion to suppress evidence obtained against Duggan, a U.S. citizen, who was never a formal target for FISA surveillance).

<sup>224</sup> *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 321-24 (1967), cited in *Duggan*, 743 F.2d at 72 ("[T]he warrant requirement is flexible and that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations of domestic national security surveillances.").

know that they have been, or are under, FISA surveillance.<sup>225</sup> Unlike Title III criminal surveillance requirements, the government need never disclose its activities to a current or former target.<sup>226</sup> The theory is that, while prosecuting a target who is a threat to national security may be one way to reduce the security threat, often a better way is *not* to prosecute, but to continue receiving intelligence from the target, or to attempt to “double” the target or feed him false information.<sup>227</sup> Thus, only if the government (i) voluntarily discloses such information, or (ii) brings a criminal action against a target, or against someone incriminated by evidence obtained through the target (like Duggan above), will any person be made aware of the surveillance.<sup>228</sup> However, even in criminal actions defendants for practical purposes are never allowed access to the original FISA application in order to contest its issuance.<sup>229</sup> In

---

<sup>225</sup> See, e.g., *U.S. Patriot Act Authorization: Hearing to Clarify Definition in the Foreign Intelligence Surveillance Act of 1978 Before the Sen. Select Comm. on Intelligence*, 109th Cong. 1 (2005) (testimony of Joseph Onek, Senior Policy Analyst, Open Society Institute, Senior Counsel, Constitution Project Senate Select Committee on Intelligence) (hereinafter Onek Testimony), available at [http://www.fas.org/irp/congress/2005\\_hr/052405onek.html](http://www.fas.org/irp/congress/2005_hr/052405onek.html).

[T]he government can obtain an order to conduct secret searches of any home or office. . . . [T]hese searches remain secret forever unless the government chooses to disclose them or there is a criminal trial involving evidence seized during the search. This means that innocent Americans have had, and will have, their most intimate records and belongings searched by the government without ever being informed of the search.

*Id.* (emphasis added).

<sup>226</sup> *Id.* (“[A]lthough Title III wiretaps are ultimately disclosed, FISA wiretaps are not.”) (emphasis added).

<sup>227</sup> See H.R. REP. NO. 95-1283, pt. 1, at 36–7 (1978). Congress noted that [c]ombating the espionage and covert actions of other nations in this country is an extremely important national concern. *Prosecution is one way, but only one way and not always the best way, to combat such activities.* “Doubling” an agent or feeding him false or useless information are other ways. Monitoring him to discover other spies, their tradecraft and equipment can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to find or whom may never be found.

*Id.* (emphasis added).

<sup>228</sup> H.R. REP. NO. 95-1283, pt. 1, at 36–7. “[T]hese [FISA] searches remain secret forever unless the government chooses to disclose them or there is a criminal trial involving evidence seized during the search. Onek Testimony, *supra* note 225.

<sup>229</sup> See *United States v. Sattar*, No. 02 CR. 395 JGK, 2003 U.S. Dist. Lexis 16164, at \*19 (S.D.N.Y. Sept. 15, 2003) (“The Government represents that it is unaware of any court ever ordering disclosure” of contents of a FISA application.); S. REP. NO. 108-40, at 13 (2003) (reporting that “no FISA application [or] even a portion of such an application has been provided to a criminal defendant in discovery”). See also *United States v. Belfield*,

fact, no district court has ever found that disclosure to the defense was necessary to make an accurate determination of the legality of the FISA surveillance.<sup>230</sup> In sum, with respect to gaining access to FISA applications to challenge their validity, a criminal defendant in Duggan's situation has his hands tied.

When *Duggan* was decided, none of the eight legislative acts that amended FISA had been passed.<sup>231</sup> The decision in *Duggan* was made when the original FISA safeguards were still in force. While *Duggan* stands for the proposition that vicarious targets of nonresident alien surveillance may be prosecuted, today the force of that proposition may be significantly eroded because of the numerous FISA amendments post-*Duggan* that have relaxed (and arguably eliminated) the nonresident alien surveillance requirements.

### C. *The Disappearing Nonresident Alien Safeguards*

At the time FISA was enacted Congress set up "two separable categories," one for United States persons and another for nonresident aliens, with different rules governing FISA surveillance for each.<sup>232</sup> This dichotomy between United States persons and nonresident aliens manifested in reduced standards for targeting non-

---

692 F.2d 141, 149 (D.C. Cir. 1982) ("The language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary.") (emphasis in original); *United States v. Nicholson*, 955 F. Supp. 588, 592 n.11 (E.D. Va. 1997) ("[T]his court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance"); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990) ("No court that has been required to determine the legality of a FISA surveillance has found disclosure or any adversary hearing necessary."); *United States v. Ott*, 637 F. Supp. 62, 65-66 (E.D. Ca. 1986) (rejecting motion for disclosure and finding *ex parte* and *in camera* review constitutional).

<sup>230</sup> See, e.g., Brief for National Association of Criminal Defense Lawyers as Amicus Curiae in Support of Affirmance, *In re Sealed Case*, 310 F.3d 717, 717 (FISA Ct. Rev. 2002) (stating that "no district court has ever found under § 1806(f) that disclosure to the defense was necessary to make an accurate determination of the legality of the surveillance; and no court of appeals has ever reversed a district court's decision to deny defense access to FISA materials under § 1806(f)") (internal quotes omitted). In practice, § 1806(f) has completely barred defense counsel from access to the application and other materials underlying FISA orders issued by the FISC. *Id.*

<sup>231</sup> For a list of the eight legislative rounds of amendments to FISA, see *supra* note 196. For a discussion of the amendments, see *supra* Parts II.C and III.D.

<sup>232</sup> See H.R. REP. NO. 95-1283, pt. 1, at 32 (noting that FISA creates "two separable categories" and that "protections afforded [nonresident aliens] are not as great as those afforded United States persons").

2007]

## DISAPPEARING SAFEGUARDS

211

resident aliens.<sup>233</sup> Congress stated that these distinctions between the two groups were constitutional, but cautioned that the distinctions must be “reasonable in light of the demonstrated need and not be overly broad.”<sup>234</sup>

Congress enacted FISA in 1978 with the following requirements. (1) For a United States person, the government was required to provide probable cause that the target had been or was about to be involved in the commission of a crime.<sup>235</sup> No criminal standard was required for targeting a nonresident alien under FISA.<sup>236</sup> (2) FISA required the government to minimize the acquisition, retention and dissemination of sensitive information on United States persons.<sup>237</sup> By contrast, minimization requirements did not exist for information acquired on nonresident alien wiretaps.<sup>238</sup> (3) Judicial approval of a FISA warrant required that a FISA judge review the government’s application for clear error.<sup>239</sup> By contrast, “no judge reviews the executive certification when [nonresident aliens] are targeted.”<sup>240</sup> (4) Congress noted that whereas emergency orders targeting a United States person required a FISA warrant, such orders against nonresident aliens would not require a warrant at all.<sup>241</sup>

Thus, with no probable cause requirement, no minimization requirement, no judicial review, and no warrant required in emergencies, the threshold for acquiring a FISA warrant for nonresident aliens was already lower than the threshold for United States

---

<sup>233</sup> *Id.* See also *infra*, notes 236–241.

<sup>234</sup> H.R. REP. NO. 95-1283, pt. 1, at 33.

<sup>235</sup> *Id.* (“As a matter of principle, this Committee agrees that no United States citizen in the United States should be targeted for electronic surveillance by his government absent some showing that he at least may violate the laws of our society.”).

<sup>236</sup> *Id.* at 32 (“The standard for targeting nonresident aliens does not have a criminal standard.”). See also Original FISA 1978, Pub. L. No. 95-511, § 101(b)(1), 92 Stat. 1783, 1783–1784 (1978) (codified as amended at 50 U.S.C. § 1801(b)(1) (1978)) (containing no criminal requirements). The so-called “may involve” and “about to involve” FISA standards, the criminal standard, and probable cause are discussed *supra* Part II.B.1.

<sup>237</sup> See Original FISA 1978 § 101(h) (codified as amended at 50 U.S.C. § 1801(h) (1978)).

<sup>238</sup> See H.R. REP. NO. 95-1283, pt. 1, at 32 (stating that “there is no requirement to minimize the acquisition, retention, and dissemination of information with respect to [nonresident aliens].”); 50 U.S.C. § 1801(h) (2006) (containing no minimization requirement for nonresident aliens).

<sup>239</sup> See 50 U.S.C. § 1805(a)(5) (2006); see also *In re Sealed Case*, 310 F.3d 717, 739 (FISA Ct. Rev. 2002).

<sup>240</sup> H.R. REP. NO. 95-1283, pt. 1, at 32.

<sup>241</sup> See *id.*; see also 50 U.S.C. § 1801(f) (2006) (defining “emergency orders”).

persons. However, Congress still retained two important safeguards for nonresident aliens. The government had to (1) certify that the primary purpose for the surveillance was to obtain foreign intelligence information,<sup>242</sup> and (2) establish a nexus between the target and a foreign power.<sup>243</sup> Additionally, FISA imposed an administrative requirement that the application be made by a federal officer and approved by the Attorney General.<sup>244</sup>

The first retained safeguard, the primary purpose requirement, was abolished in 2001 when the Patriot Act was passed.<sup>245</sup> The second retained safeguard, nexus with a foreign power, was eliminated when the Lone Wolf Amendment passed in 2004.<sup>246</sup> Thus, today, none of the original safeguards remains. Furthermore, Congress has begun to enlarge the existing FISA authority over nonresident alien FISA orders by extending the duration of such orders.<sup>247</sup> For a nonresident alien FISA warrant, if the application is made by a federal officer and approved by the Attorney General, satisfying a mere administrative requirement, then the FISC “shall enter an *ex parte* order” granting the warrant.<sup>248</sup>

#### D. *Adding Up the FISA Amendments*

The original FISA covered only wiretapping.<sup>249</sup> Physical searches were added in 1994,<sup>250</sup> pen register and trap and trace ad-

---

<sup>242</sup> See Original FISA 1978 § 104(a)(7)(B) (codified as amended at 50 U.S.C. § 1804(a)(7)(B) (1978)).

<sup>243</sup> See Original FISA 1978 § 101(b)(1) (codified as amended at 50 U.S.C. § 1801(b)(1) (1978)) (requiring a nexus with a foreign power for all targets, both United States person targets and nonresident alien targets). See also S. REP. NO. 95-604, at 21 (1978) (“The alien must be engaged in ‘clandestine intelligence activities’ for or on behalf of a foreign power.”).

<sup>244</sup> See Original FISA 1978 § 105(a)(2) (codified as amended at 50 U.S.C. § 1805(a)(2) (1978)). When nonresident aliens are targeted, no judge reviews the Attorney General’s certification. See *supra* note 240.

<sup>245</sup> Patriot Act, Pub. L. No. 107-56, § 218, *115 Stat. 272, 291 (2001)* (codified at 50 U.S.C. § 1804(a)(7)(B)). See also *supra* Parts II.B.2 and II.C.1.

<sup>246</sup> See *supra* notes 176–177.

<sup>247</sup> See discussion on the USA PATRIOT Improvement and Reauthorization Act of 2005, *supra* Part II.C.3.

<sup>248</sup> See 50 U.S.C. § 1805 (2006).

<sup>249</sup> See Original FISA 1978 §§ 101–111 (codified as amended at 50 U.S.C. §§ 1801–1811 (1978)).

<sup>250</sup> See Physical Searches Amendment 1994, Pub. L. No. 103-359, tit. VIII, § 807(a)(1), (2), 108 Stat. 3423, 3443 (1994) (codified as amended at 50 U.S.C. §§ 1821–1829) (codifying Physical Searches within the United States for Foreign Intelligence Purposes).

R

R

ditions were made in 1998,<sup>251</sup> the definition of “agent of a foreign power” was expanded in 1999,<sup>252</sup> and language intended to increase the thoroughness and effectiveness of investigations was added in 2000.<sup>253</sup> All of these additions have increased the Executive’s ability to conduct surveillance under FISA. As the Executive’s powers to obtain FISA warrants increase, so does the reach of the nonresident alien loophole.

In 2001 the Patriot Act abolished the first major substantive nonresident alien requirement, the primary purpose requirement, by enacting eight sections that drastically increased the scope of the Executive’s power under FISA.<sup>254</sup> In particular, section 218 of the Patriot Act eliminated the primary purpose requirement and changed it to “a significant purpose.”<sup>255</sup> Under the primary purpose regime, many potential FISA targets were pre-screened in the field or at FBI headquarters, never even making it to the FISC for approval.<sup>256</sup> Restricting nonresident alien wiretaps to primarily

<sup>251</sup> See Pen Register Amendment 1998, Pub. L. No. 105-272, tit. VI, §§ 601(1), 603(a), 112 Stat. 2404, 2412 (1998) (codified as amended at 50 U.S.C. §§ 1841–1846 (1998)) (codifying pen register, trap and trace legislation under FISA).

<sup>252</sup> See Agent of a Foreign Power Amendment, 1999, Pub. L. No. 106-120, tit. VI, § 601, 113 Stat. 1606, 1619 (1999) (codified as amended at 50 U.S.C. § 1801(b)(2)(D)) (expanding the definition of “agent of a foreign power” to include “any person who . . . knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power”).

<sup>253</sup> See Counterintelligence Reform Act of 2000, Pub. L. No. 106-567, title VI, § 601, 114 Stat. 2831, 2850 (codified as amended in various sections of 50 U.S.C.). The legislation required that

upon the request of the Director of the FBI, the Secretary of State, the Secretary of Defense or the Director of Central Intelligence, the Attorney General shall personally review a FISA application. If the Attorney General decides not to forward the application to the FISA court, that decision must be communicated in writing to the requesting official, with recommendations for improving the showing of probable cause, or whatever defect OIPR is concerned with.

146 CONG. REC. S9686 (daily ed. Oct. 3, 2000) (remarks of Sen. Specter), *available at* [http://www.fas.org/irp/congress/2000\\_cr/s100300a.html](http://www.fas.org/irp/congress/2000_cr/s100300a.html).

<sup>254</sup> For a list of the eight rounds of FISA amendments, see *supra* note 196. For a discussion of the amendments, see *supra* Parts II.C and III.D.

<sup>255</sup> Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001) (codified at 50 U.S.C. § 1804(a)(7)(B)).

<sup>256</sup> INTERIM REPORT ON FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMM.: FISA IMPLEMENTATION FAILURES, 107TH CONG., § III(C)(4): The Working Relationship Between FBI Headquarters and Field Offices (Feb. 25, 2003), [http://www.fas.org/irp/congress/2003\\_rpt/fisa.html](http://www.fas.org/irp/congress/2003_rpt/fisa.html) [hereinafter INTERIM REPORT: FBI IMPLEMENTATION FAILURES] (“Under the system designed by the FBI, a field agent and his field supervisors must negotiate a series of bureaucratic levels in order to even ask for a FISA warrant.”).

foreign intelligence gathering operations, to comply with the primary purpose test, significantly narrowed the available class of people affected by the nonresident alien loophole.<sup>257</sup> Part of Congress' calculus in assessing the constitutionality of FISA's alienage distinctions was that the purpose provision would help impose a limit on the scope of available targets.<sup>258</sup>

The second major substantive nonresident alien requirement, nexus with a foreign power, was discarded when the Lone Wolf amendment was passed in 2004. The amendment was seen as a "Moussaoui Fix" and was enacted to respond to fears that the government was ill-equipped to combat terrorists acting alone.<sup>259</sup> Like the "significant purpose" provision, the Lone Wolf Amendment's effect on the nonresident alien loophole was largely, if not completely, overlooked. Senators Leahy and Feingold continued to caution generally, but the specific erosion of nonresident alien safeguards appears to have been missed by congressional radar.<sup>260</sup>

Roving wiretaps were added to FISA by section 206 of the Patriot Act.<sup>261</sup> The intent was to help FISA keep pace with tech-

---

<sup>257</sup> See H.R. REP. NO. 95-1283, pt. 1, at 36 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf> ("[T]his committee recognizes full well that the surveillance under this bill are not primarily for the purpose of gathering evidence of a crime."). See also 147 CONG. REC. S10593 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy), cited in *In re Sealed Case*, 310 F.3d 717, 733 (FISA Ct. Rev. 2002) (finding it "very problematic" that the Patriot Act would "make it easier for the FBI to use a FISA wiretap . . . where the government's most important motivation for the wiretap is for use in a criminal prosecution").

<sup>258</sup> See, e.g., S. REP. NO. 95-604, at 21, 22 (1978) (stating that the nonresident alien "must be engaged in . . . [activities] harmful to the security of the United States.") (emphasis added). See also H.R. REP. NO. 95-1283, pt. 1, at 36. But see *supra* notes 161-175 and accompanying text (debate about whether Congress intended to implement a primary purpose test).

<sup>259</sup> See discussion *supra* Part II.C.2.

<sup>260</sup> See S. REP. NO. 108-40, at 6 n.3 (2003) (quoting Senator Feingold) (cautioning generally that the Lone Wolf Amendment "writes out of the statute a key requirement necessary to the lawfulness of such searches"). Senator Leahy joined Senator Feingold in expressing broad concerns about the Lone Wolf Amendment.

We are all against terrorism. The unanswered question is whether the Congress will take real steps to ensure that the FBI and DOJ are not underusing, overusing or misusing the power that they already have and which we expanded in the USA PATRIOT Act. We must write fewer blank checks to the Executive Branch and instead focus more on ensuring that our constitutional system of checks and balances is enforced.

S. REP. NO. 108-40, at 12. The Senators noted further that "Congress, while being kept in the dark, is being asked instead to expand the FISA statute still further." S. REP. NO. 108-40, at 11.

<sup>261</sup> See *supra* note 124.

R

R

nology and defeat tactics to evade surveillance such as rapidly switching cell phones.<sup>262</sup> Roving wiretaps allow the government to create anonymous “John Doe” wiretaps, without specifying the target, or the place to be wiretapped, which increases the likelihood that conversations of innocent people wholly unrelated to an investigation will be intercepted.<sup>263</sup> Coupled with the exceedingly low nonresident alien standard, a “John Doe” roving wiretap on a nonresident alien could easily be used to obtain information on a United States person in derogation of the FISA minimums.

### E. *Constitutional Concerns*

The Supreme Court has determined that reasonableness is the touchtone of the Fourth Amendment, requiring an assessment of the interests of the government against the rights of the individual.<sup>264</sup> In defending national security, the government has an inter-

---

<sup>262</sup> See *supra* notes 124–126.

<sup>263</sup> See 149 CONG. REC. S12387 (daily ed. Oct. 2, 2003) (statement of Sen. Craig), available at [http://www.fas.org/irp/congress/2003\\_cr/s1709.html](http://www.fas.org/irp/congress/2003_cr/s1709.html). Sen. Craig introduced several hypotheticals which explained the harm in authorizing roving wiretaps. The hypotheticals were given in the context of support for the SAFE Acts which would have imposed limitations on executive wiretapping. *Id.* See H.R. 1526, 109th Cong. (2005) (introduced by Rep. Otter); S. Res. 737, 109th Cong. (2005) (introduced by Sen. Craig) (collectively the SAFE Acts). For example, Sen. Craig explained how roving wiretaps would allow over-inclusive wiretapping.

[Suppose] [t]he FBI is tracking a suspected terrorist who is using public phones at local restaurants to do business. The PATRIOT Act would permit the issuance of a roving wiretap that would apply to any phone the suspect uses. Under the PATRIOT Act, the FBI could monitor the conversations not just of the suspect, but of innocent patrons of these restaurants. The SAFE Act would also permit the issuance of a roving wiretap that would apply to any phone the suspect uses, but would only permit the FBI to gather intelligence when they ascertain that the suspect is using a phone.

S. Res. 737. Sen. Craig also suggested another possibility.

[Suppose] [t]he FBI is investigating suspected members of a terrorist cell and would like to subpoena the records of a library and a bookstore that they frequent. Currently, the FBI could subpoena all of the records of the library and bookstore, including the records of countless innocent Americans, by certifying they are sought for a terrorism investigation, the exceedingly low standard created by the PATRIOT Act. The SAFE Act would permit the FBI to obtain the records related to the suspected terrorists, but not records related to innocent Americans who are not suspected terrorists.

*Id.*

<sup>264</sup> *United States v. Knights*, 534 U.S. 112, 118–19 (2001) (“The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined ‘by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.’” (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999))).

est in thwarting acts of subversion and terror—an interest which may conflict with privacy and free expression when secret wiretapping or other surveillance techniques are employed.<sup>265</sup> Whereas there is deference under the national security exception for defending and protecting the nation,<sup>266</sup> the ability to conduct searches and seizures in the name of national security is not absolute.<sup>267</sup> The Supreme Court has suggested, for example, that unilateral executive action, accompanied by no meaningful review or oversight, would violate the Fourth Amendment.<sup>268</sup> In *Doe v. Ashcroft*, an electronic search and seizure law that had been amended by the Patriot Act was held unconstitutional because it allowed unilateral governmental power over disclosure of targeted electronic communications without any form of judicial process or protection.<sup>269</sup> In *Berger v. New York*, the Supreme Court struck down a state eavesdropping law due to its sweeping language allowing “general searches.”<sup>270</sup> In light of these Fourth Amendment concerns, when FISA was enacted, Congress required that alienage distinctions be reasonable and not overly broad.<sup>271</sup>

<sup>265</sup> See *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 314–15 (1967) (“[O]ur task is to examine and balance 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.”).

<sup>266</sup> See *supra* note 30 (discussion of national security exception).

<sup>267</sup> See, e.g., *Keith*, 407 U.S. at 314–15 (“[T]he Fourth Amendment is not absolute in its terms.”).

<sup>268</sup> *Id.* at 317 (“The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.”).

<sup>269</sup> See *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004) (holding 18 U.S.C. § 2709 unconstitutional because it afforded the FBI “extraordinary and unchecked power to obtain private information without any form of judicial process”). The Court concluded that

§ 2709 violates the Fourth Amendment because, at least as currently applied, it effectively bars or substantially deters any judicial challenge to the propriety of an NSL request. In the Court’s view, ready availability of judicial process to pursue such a challenge is necessary to vindicate important rights guaranteed by the Constitution or by statute.

*Id.* See also discussion *infra* note 280.

<sup>270</sup> *Berger v. New York*, 388 U.S. 41, 44 (1967) (“[T]he language of New York’s statute is too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area and is, therefore, violative of the Fourth and Fourteenth Amendments.”).

<sup>271</sup> See H.R. REP. NO. 95-1283, pt. 1, at 33 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf>. The Committee wrote:

The basic test under the fourth amendment is that a search be reasonable. . . . [Foreign intelligence] information by definition must directly and substantially

R

R

Today, the nonresident alien loophole leaves a gaping hole where Congress originally imposed sufficient safeguards.<sup>272</sup> The government may target nonresident aliens with no meaningful judicial process or congressional oversight.<sup>273</sup> No showing of any probable cause is required, no showing of a nexus with a foreign power is required, and no requirement exists to prohibit governmental wiretaps whose primary purpose is a criminal conviction.<sup>274</sup> The full force of the criminal justice system may be used against by-

---

relate to important foreign policy or national security concerns, and high Executive officials must certify that the purpose of the surveillance is to obtain such information.

*Id.*

<sup>272</sup> See S. REP. NO. 95-604, at 20–21 (1978) (carefully demarking the class of nonresident aliens and the prerequisites for securing a nonresident alien FISA warrant).

Subparagraph (A)(ii) defines an agent of a foreign power as a person who is not a citizen or resident alien of the United States who “knowingly engages in clandestine intelligence activities for or on behalf of a foreign power under circumstances which indicate that such activities would be harmful to the United States.” This category could potentially include illegal aliens, foreign terrorists, exchange visitors, foreign businessmen, foreign students, and foreign seamen.

*Id.* The House Select Committee on Intelligence described the class of nonresident aliens as “limited.” See H.R. REP. NO. 95-1283, pt. 1, at 32. The committee also specifically tailored the nonresident alien category to the “demonstrated need” made by the government. *Id.* at 33. The Committee “exclude[d] persons who serve as officers or employees or are members of a foreign power in their home country, but do not act in that capacity in the United States.” *Id.* at 34. Today, there would be no bar to targeting any of these formerly excluded persons under Lone Wolf authority. See Lone Wolf Amendment Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004) (codified as amended at 50 U.S.C. § 1801(b)(1)(C)) (2005).

The class of nonresident aliens was originally “not intended to encompass such foreign visitors [who are] professors, lecturers, exchange students, performer [sic] or athletes, even if they are receiving remuneration or expenses from their home government in such capacity.” 140 CONG. REC. S2883, S2894, *Counterintelligence Improvement Act of 1994 Section-by-Section Analysis* (daily ed. Mar. 11, 1994), available at [http://www.fas.org/irp/congress/1994\\_cr/s940311-ci.htm](http://www.fas.org/irp/congress/1994_cr/s940311-ci.htm). Again, because the Lone Wolf Amendment created an incredibly easy standard for targeting nonresident aliens, requiring merely that the nonresident alien engage in or be *preparing to engage in* “international terrorism,” the government would be able to target these individuals noted above that Congress originally intended to exclude. See Lone Wolf Amendment.

Finally, the Committee defined “member” to mean “an active, knowing member of the group or organization which is engaged in international terrorism or activities in preparation therefor.” *Id.* The Lone Wolf Amendment allows the government to target all of these individuals today. Lone Wolf Amendment. Thus, by eliminating the nexus with a foreign power requirement, the Lone Wolf Amendment opened up surveillance to carefully excluded groups of persons. Other FISA amendments act in concert with the Lone Wolf Amendment to eliminate the remaining meaningful limits originally imposed by Congress for targeting nonresident aliens. See *supra* Parts III.C., III.D.

<sup>273</sup> See *supra* Part III.C.

<sup>274</sup> See *supra* notes 242–248 and accompanying text.

standers.<sup>275</sup> There is likewise no process for challenging potential abuses or mistakes.<sup>276</sup> There is no safeguard against the government purposefully targeting a nonresident alien and conducting a “fishing expedition” on United States citizens.<sup>277</sup> Furthermore, abuses and mistakes are a reality in the FBI.<sup>278</sup> Why should the FBI be trusted to behave?

Today, FISA surveillance on a nonresident alien imposes little more than a filing requirement.<sup>279</sup> In examining and balancing the basic values at stake, individuals face irreparable harm for wrong convictions based on secret evidence and a disturbing intrusion of the fundamental right to privacy. The government’s general interest in preventing terror must be weighed against the unilateral methods it has acquired for targeting nonresident aliens. The reasonableness requirement of the Fourth Amendment requires that Congress reexamine the nonresident alien loophole and consider safeguards that would implement minimal process or oversight.

#### F. *Possible Remedies*

The court in *Doe v. Ashcroft* stated that “[s]ometimes a right, once extinguished, may be gone for good.”<sup>280</sup> It is important to

---

<sup>275</sup> See, e.g., *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); discussion *supra* notes 215–230.

<sup>276</sup> See *supra* Part III.C.

<sup>277</sup> See *supra* Part III.C.

<sup>278</sup> See Dan Eggen, *FBI Cites More Than 100 Possible Eavesdropping Violations*, Mar. 9, 2006, [http://www.washingtonpost.com/wpdyn/content/article/2006/03/08/AR2006030802132\\_pf.html](http://www.washingtonpost.com/wpdyn/content/article/2006/03/08/AR2006030802132_pf.html). In a self-administered evaluation, the FBI reported that in the last two years more than 100 possible eavesdropping violations have occurred in which agents tapped the wrong telephone, intercepted the wrong e-mails or continued to listen to conversations after a warrant had expired. In one case, the FBI obtained the contents of 181 telephone calls rather than just the billing records to which it was entitled. In another, a communication was monitored for more than a year after eavesdropping should have ended.

*Id.*

<sup>279</sup> See *supra* note 248 and accompanying text.

<sup>280</sup> *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 477 (S.D.N.Y. 2004). In September 2004, the Southern District of New York held section 505 of the Patriot Act unconstitutional. *Id.* at 526–27. (“[T]he Court concludes that the compulsory, secret, and unreviewable production of information required by the FBI’s application of 18 U.S.C. § 2709 [as amended by section 505 of the Patriot Act] violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment.”). The court found that section 505, which expanded powers under the Electronic Communications Privacy Act (ECPA), violated the First Amendment because it prohibited recipients of National Security Letters (NSLs), including the recipient’s officers, employees, and agents, from revealing the existence of an NSL inquiry, in perpetuity. *Id.* at 476. The court found that the section

R

R

reexamine the diminished nonresident alien provisions and to guard against incremental encroachment upon our liberties. In 1978, the government demonstrated a legitimate need to be able to target nonresident aliens more quickly and with less oversight.<sup>281</sup> The legislative history reports that this “need has been demonstrated to this committee in testimony before it.”<sup>282</sup> Remember, however, that reduced nonresident alien standards were adopted in the context that a nexus with a foreign power would be required.<sup>283</sup> A very careful balance was struck by Congress, which it believed satisfied the Constitution.<sup>284</sup>

In order to eliminate the problems created by the nonresident alien loophole, there are several possible solutions. (1) Statutory language could be included to require a parallel application to be filed, under the regular standards, if the government reasonably believed information on a United States person would be collected. This method would preserve the distinctions between nonresident aliens and United States persons, allowing nonresident alien warrants to be issued for the narrow purpose of gathering evidence on that alien. The ability to circumvent the United States person safeguards would be foreclosed by requiring the government to obtain a parallel warrant for United States persons.

The problem with this solution is the excessive burden on the government to make and file precautionary parallel warrants. Filing parallel applications would require the government to speculate unnecessarily on whether United States persons would potentially be intercepted in the surveillance.

(2) Another solution would be to require the government to return to the FISC for approval each time evidence from a United States person was intercepted by a nonresident warrant. This solution would obviously create undue administrative burdens. Offi-

---

violated the Fourth Amendment because it barred “any judicial challenge to the propriety of an NSL request.” *Id.* at 475. At this writing, *Doe v. Ashcroft* represents the only successful constitutional challenge to the Patriot Act. *Doe v. Ashcroft* is currently under appeal.

<sup>281</sup> H.R. REP. NO. 95-1283, pt. 1, at 33 (1978), available at <http://www.cnss.org/rpt%2095-1283pt1.pdf> and <http://www.cnss.org/rpt%2095-1283pt2.pdf>; see also discussion *supra* notes 203–207 and accompanying text.

<sup>282</sup> H.R. REP. NO. 95-1283, pt. 1, at 33.

<sup>283</sup> *Id.* In the legislative history, the acknowledgment of the government’s need for reduced nonresident alien safeguards was preceded in the very same sentence by an acknowledgement the nonresident alien be linked to a foreign power. *Id.*

<sup>284</sup> *Id.*

cials would have to continually monitor and interpret information coming in from nonresident alien wiretaps, separate out and determine, in real time, what information would potentially implicate a United States person, make judgment calls on what to do with information that might implicate *both* nonresident aliens and United States persons, and decide what to do with information where the implication might not be clear. Requiring a new application or approval each time a United States person is implicated on a nonresident alien warrant would also involve undoing many years of precedent allowing such information to be lawfully collected.

(3) Congress could eliminate the distinctions between nonresident aliens and United States persons and implement a uniform standard. The benefits would be immediate increased safeguards for United States persons and a complete closing of the nonresident alien loophole. The drawbacks would be increased hurdles for the government in the sensitive area of national security. Additionally, as reported when FISA was enacted, a legitimate need for alienage distinctions had been demonstrated.<sup>285</sup> Such a power shift, removing important tools at the government's disposal for detecting and removing terrorist threats, seems especially unlikely and unworkable in an age of national security crisis.

(4) A final solution would be to implement regular oversight and reporting requirements. For example, currently there is no reporting requirement that the government keep track of how many active FISA targets are nonresident aliens.<sup>286</sup> There is also no requirement that the government document how many criminal prosecutions against United States citizens are brought up on secret evidence obtained vicariously through nonresident alien wiretaps.<sup>287</sup> These minimal reporting requirements should be

---

<sup>285</sup> *Id.* at 33–34.

<sup>286</sup> See, e.g., AMERICAN BAR ASSOCIATION, SECTION OF INDIVIDUAL RIGHTS AND RESPONSIBILITIES: REPORT TO THE HOUSE OF DELEGATES 1 (2003), <http://www.abanet.org/leadership/recommendations03/118.pdf> (urging Congress to conduct better public reporting regarding FISA).

<sup>287</sup> See INTERIM REPORT: FBI IMPLEMENTATION FAILURES, *supra* note 256, § IV. The Importance of Enhanced Congressional Oversight (giving a negative assessment of required reporting under FISA).

Under current law there is no requirement that FISA Court opinions be made available to Congressional committees or the public. The only statutory FISA reporting requirement is for an unclassified annual report of the Attorney General to the Administrative Office of the United States Courts and to Congress setting forth with respect to the preceding calendar year (a) the total number of applications made for orders and extensions of orders approving electronic sur-

mandatory.<sup>288</sup> In addition, there should be a vehicle for reviewing and determining whether the government has attempted to circumvent the FISA requirements by targeting a nonresident alien.<sup>289</sup>

#### IV. CONCLUSION

Today, of the original safeguards adopted for nonresident alien wiretapping, only the administrative requirements remain.<sup>290</sup> This relaxation of nonresident alien wiretapping standards exaggerates the nonresident alien loophole, and puts United States persons at risk.<sup>291</sup> The nonresident alien loophole enables the government to target a nonresident alien under reduced standards and use the fruits of that surveillance to bring a criminal prosecution against a United States person. As originally enacted, FISA imposed safeguards on nonresident alien wiretapping, which confined the nonresident alien loophole to a very narrow group of situations.<sup>292</sup> Due to the recent amendments to FISA, the once narrow nonresident alien loophole expanded beyond constitutional limits.<sup>293</sup>

Reexamination of the nonresident alien loophole is necessary. Several solutions have been examined, and costs to these solutions considered. It is important to remember that the potential for a national security emergency is distressingly high at this time.<sup>294</sup> We all wish to empower the government to swiftly and secretly infiltrate and apprehend our enemies. Yet, valuable individual liberties

---

veillance under Title I, and (b) the total number of such orders and extensions either granted, modified, or denied. *These reports do not disclose or identify unclassified FISA Court opinions or disclose the number of individuals or entities targeted for surveillance, nor do they cover FISA Court orders for physical searches, pen registers, or records access.*

*Id.* (emphasis added).

<sup>288</sup> See *supra* notes 286–287.

<sup>289</sup> See generally INTERIM REPORT: FBI IMPLEMENTATION FAILURES, *supra* note 256, § I. Executive Summary and Conclusions (stating that “corrective actions” are an “important purpose of oversight”). The Committee found that “[w]ith those enhanced powers [from the Patriot Act] comes an increased potential for abuse and the necessity of enhanced congressional oversight.” *Id.*

<sup>290</sup> See *supra* notes 242–246; Part III.D.

<sup>291</sup> See, e.g., *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); discussion *supra* notes 215–230.

<sup>292</sup> See *supra* note 272.

<sup>293</sup> See *supra* Part III.E.

<sup>294</sup> See Homeland Security, Threats and Protection, <http://www.dhs.gov/dhspublic/display?theme=29> (last visited Jan. 24, 2007) (stating that the current threat level is “high” signifying a “high risk of terrorist attacks”).

R

R

R

R

R

222 *CARDOZO J. OF INT'L & COMP. LAW* [Vol. 15:169]

are often lost to “emergency powers.”<sup>295</sup> It is with this knowledge that we must revisit the disappearing safeguards and reexamine the nonresident alien loophole.

---

<sup>295</sup> See, e.g., *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 653 (1952) (Jackson, J., concurring) (cautioning that emergency powers have neither a beginning nor an end); *Eachus v. People*, 124 Colo. 454, 471–72 (1951).

Under the stress and strain of war and other so-called national emergencies, appellate courts in recent strenuous years have been inclined to emasculate constitutional provisions until basic guarantees of our constitutions, both national and state, have lost much of their original meaning. This result has been brought about in many ways, and no doubt with the best of intentions. However, if constitutional government is to survive, the creeping paralysis that has set upon the once deep rooted concepts of constitutional law must be met by appellate courts with a reaffirmance of fundamentals, and a rededication by appellate judges to the task of restoring health and vigor to our constitutional body to the end that the constitutions of our state and nation shall in actual practice amount to a first line of defense against invasions upon the freedoms and liberties of the people.

*Id.*