WHAT REALLY IS AT STAKE WITH THE FISA AMENDMENTS ACT OF 2008 AND IDEAS FOR FUTURE SURVEILLANCE REFORM

STEPHANIE COOPER BLUM[1]

ABSTRACT

The need to reconcile domestic intelligence requirements with the protection of civil liberties is a recurring and prominent theme in the war on terror. While this tension between domestic intelligence gathering and civil liberties can be seen in many contexts since 9/11, this Article focuses on the Bush administration's Terrorist Surveillance Program (TSP), where the National Security Agency (NSA) secretly wiretapped Americans without traditional Foreign Intelligence Surveillance Act (FISA) warrants and the resulting FISA reform legislation culminating in the FISA Amendments Act of 2008 (FAA). In July 2008, the American Civil Liberties Union (ACLU) filed suit against the FAA arguing that it is unconstitutional; this Article, however, argues that the FAA is most likely lawful and appears to be a nuanced compromise between the legitimate need to expeditiously gather intelligence against terrorists and the protection of Americans' civil liberties. In order to draw this conclusion, it is necessary to understand what traditional FISA requires, how the TSP program departed from that rubric, and how advances in technology and the nature of terrorism have impacted intelligence gathering.

Part I of this Article analyzes the legal framework of domestic spying and discusses the Fourth Amendment, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, FISA, and changes made to FISA with the USA Patriot Act. Part II analyzes the Bush administration's warrantless surveillance program and whether, and to what extent, it violated the

[1] Stephanie Cooper Blum works as an attorney for the Transportation Security Administration, Department of Homeland Security. She is currently on a detail to the Department of Justice. Ms. Blum holds a M.A. in security studies from the U.S. Naval Postgraduate School's Center for Homeland Defense and Security, a J.D. from The University of Chicago Law School, and a B.A. in political science from Yale University. She has published a book and various articles on homeland security issues. She would like to thank Professor Robert Chesney and the participants at the annual national security law junior faculty workshop for their suggestions. The views in this article are the author's and do not necessarily represent the views of the U.S. Government to include the Department of Homeland Security and Department of Justice.

law. Part III discusses the challenges posed by terrorism to intelligence gathering and the need for modifications to FISA. Part IV analyzes the FAA of July 2008 and ponders whether it is just the perception that civil liberties could be eroded, or whether Americans' civil liberties truly are at risk. Finally, in Part V, this Article argues that in some ways the FAA has not gone far enough in addressing the underlying problems with conducting surveillance of terrorists and suggests areas for future reform.

INTRODUCTION

"[A]ny time you hear the United States government talking about wiretap, it requires . . . a court order. Nothing has changed. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so."

President George W. Bush, 2004[2]

President Bush made this statement to the public in 2004. Just one year later, the *New York Times* revealed that the Bush administration was engaging in a secret warrantless wiretap program entitled the Terrorist Surveillance Program (TSP) that targeted Americans' international communications with alleged al-Qaeda terrorists.[3] While it is easy to condemn the Bush administration for misleading the American public and engaging in what many prominent policy makers and law professors believe was unlawful surveillance of Americans, a responsible analysis must ask why the administration felt it was so imperative to bypass the Foreign Intelligence Surveillance Act (FISA) and engage in warrantless surveillance of Americans. Despite the excoriation in the press and by various lawmakers,[4] the upshot of the TSP was neither the prosecution of any government officials for ostensible violations of the law (although presumably that could still occur), nor a congressional directive to cut off funding to the National Security Agency (NSA) that engaged in the warrantless surveillance. Rather, the upshot was FISA reform legislation that addressed, in part, some of the underlying reasons why the Bush administration felt it needed a secret warrantless wiretapping program. While many articles have been written that address the illegality of the TSP[5] – and this Article addresses those arguments as

---

[2] President's Remarks in a Discussion on the Patriot Act in Buffalo, New York, 40 Weekly Comp. Pres. Doc. 641 (Apr. 20, 2004).

[3] James Risen & Eric Lichtblau, *Bush Lets U.S Spy on Callers Without Courts*, N.Y. TIMES, Dec 16, 2005.

[4] *See, e.g.*, Editorial, *The Power to Spy*, WASH. POST, Dec. 25, 2005, at B06; Donna Leinwand, *Senators Press Gonzales on Delay in Getting Court Okay on Surveillance*, USA TODAY, Jan. 19, 2007, at 4A; Eric Lichtblau, *With Power Set to Be Split, Wiretaps Re-emerge as Issue*, N.Y. TIMES, Nov. 10, 2006, at A28.

[5] *See, e.g.*, Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Cong. Research Serv., Presidential Authority to Conduct Warrantless Electronic Sur-

background – the crux of this Article is to evaluate the FISA Amendments Act of 2008 (FAA),[6] which is an outgrowth of the TSP. This Article concludes that while there is potential for abuse if government officials violate the clear wording of the FAA, which allows warrantless surveillance to gather foreign intelligence from non-US persons reasonably believed to be outside the United States, the FAA contains enough ex post review mechanisms (in the forms of Congressional oversight committees, the Foreign Intelligence Surveillance Court, and various inspectors general), that the Obama administration should allow the FAA to operate as-is, and reevaluate its effectiveness and ability to protect civil liberties when it expires in 2012. This Article further argues that in some ways the FAA has not gone far enough in addressing the underlying problems with conducting surveillance of terrorists and suggests some areas for future reform.

I. LEGAL BACKGROUND OF DOMESTIC SPYING

A. *Fourth Amendment*

The Fourth Amendment of the Constitution provides the foundation for limiting the government's role in collecting domestic surveillance. It protects against "unreasonable searches and seizures" and requires that warrants be issued only upon "probable cause."[7] At a fundamental level, it is important to understand that the warrant and reasonableness requirements are distinct. The Supreme Court has recognized situations where warrants are not required to conduct a search and seizure because the circumstances are otherwise reasonable, and it would be impractical to obtain a warrant. Examples of warrantless searches include the plain view doctrine,[8] the motor vehicle exception,[9] consensual searches,[10] searches incident to arrest,[11] and searches in exigent circum-

---

veillance to Gather Foreign Intelligence Information 12 (Jan. 5, 2006); David Cole, *Reviving the Nixon Doctrine: NSA Spying, the Commander-in-Chief, and Executive Power in the War on Terror*, 13 WASH. & LEE J. C.R. & SOC. JUST. 17 (Fall 2006); JOHN CARY SIMS, *What NSA is Doing . . . and Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105, 126-27 (2005-06).

[6] FISA Amendments Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463, 2473 (2008).

[7] U.S. CONST. amend. IV.

[8] Horton v. California, 496 U.S. 128, 133 (1990) (Fourth Amendment does not prohibit warrantless seizure of evidence of crime in plain view).

[9] Pennsylvania v. Labron, 518 U.S. 938, 940 (1996) (per curiam) (if car is readily mobile and probable cause exists to believe it contains contraband, Fourth Amendment permits police to search vehicle without a warrant).

[10] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (no warrant required if consent to search is voluntarily given).

[11] Michigan v. DeFillippo, 443 U.S. 31, 35 (1979) (lawful arrest, standing alone, authorizes a search incident to arrest).

stances.[12]

The Supreme Court has further held that a warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable."[13] In determining whether the "special needs" doctrine applies, the Supreme Court distinguishes searches designed to uncover evidence of "ordinary criminal wrongdoing" (generally requiring a warrant), and those motivated at a "programmatic level" by other governmental objectives,[14] such as stops of motorists at roadblocks for the purpose of securing the border or conducting sobriety checkpoints,[15] administrative searches in regulated industries,[16] searches of government employees to test for drugs,[17] and searches of public school students.[18] In other words, not every search and seizure requires a warrant. In *New Jersey v. T.L.O* the Supreme Court held that the "underlying command of the Fourth Amendment is always that searches and seizures be reasonable," and "what is reasonable depends on the context within which a search takes place."[19] Significantly, for purposes of this article, the Foreign Intelligence Surveillance Court of Review (FISCR) has specifically held that the government's "programmatic purpose" in obtaining foreign intelligence information is "to protect the nation against terrorist and espionage threats directed by foreign powers."[20] The "programmatic purpose" fulfills "a special need" that fundamentally differs from "ordinary crime control."[21]

---

[12] Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (under exigent circumstances, police can enter a home without a warrant).

[13] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).

[14] City of Indianapolis v. Edmond, 531 U.S. 32, 37-40, 48 (2001) (reviewing cases).

[15] United States v. Martinez-Fuerte, 428 U.S. 543, 565-66 (1976) (questioning at checkpoint near border does not require a warrant); Michigan Dept. of State Police v. Sitz, 496 U.S. 444, 453-55(1990) (stop of automobile as part of highway sobriety checkpoint program does not require a warrant).

[16] New York v. Burger, 482 U.S. 691, 708-10 (1987) (warrantless administrative inspection of premises of "closely regulated" business); Michigan v. Tyler, 436 U.S. 499, 507-509, 511-512 (1978) (administrative inspection of fire-damaged premises to determine cause of blaze); Camara v. Mun. Ct. of City and County of San Francisco, 387 U.S. 523, 534-539 (1967) (administrative inspection to ensure compliance with city housing code).

[17] Treasury Employees v. Von Raab, 489 U.S. 656 (1989) (drug tests for United States Customs Service employees seeking transfer or promotion to certain positions); Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, (1989) (drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations).

[18] Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) (random drug testing of student-athletes); New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (in-school search of student's purse).

[19] *T.L.O.*, 469 U.S. at 337 (1985).

[20] In re Sealed Case, 310 F.3d 717, 745 (For. Intel. Surv. Rev. 2002).

[21] *Id.* at 747.

Another significant fact about Fourth Amendment jurisprudence is that a governmental intrusion is only a "search" if it invades a "reasonable expectation of privacy."[22] In areas where the Supreme Court has found there to be reasonable expectations of privacy (such as private conversations), Congress has enacted two significant statutes for purposes of surveillance: Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[23] dealing with domestic wiretapping, and the Foreign Intelligence Surveillance Act (FISA),[24] which deals with the collection of foreign intelligence. An understanding of both of these statutes is fundamental background to analyze and understand what is really at stake with the FAA of July 2008.

B. *Title III*

Pursuant to the 1967 Supreme Court case *Katz v. United States*,[25] in order to conduct electronic surveillance of one's private conversations, a government agent must obtain a warrant from a judicial officer based on probable cause that criminal activity will be revealed, and the warrant must adhere to the Fourth Amendment's particularity requirements specifying the place to be searched.[26] The Court in *Katz*, however, explicitly declined to extend its holding to cases "involving the national security."[27] In 1968, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) to regulate domestic electronic surveillance to meet the Fourth Amendment's particularity requirements.[28] Congress enacted Title III to ensure that if the government obtained evidence pursuant to this statutory rubric, it would be admissible in court. Title III only allows wiretapping for certain enumerated crimes, limits the time period for the surveillance, requires minimization procedures to limit eavesdropping on innocent parties, and requires reporting to the court on the results of the surveillance.[29] In order to obtain a Title III warrant, the government official must also explain whether other investigative methods would produce the same results and specify the facilities and communications sought to be intercepted.[30]

Significantly, Title III specified that none of its provisions would "limit the constitutional power of the President to take such measures as he deems neces-

---

[22] Katz v United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[23] 18 U.S.C. §§ 2510-2522 (2006).

[24] 50 U.S.C. §§ 1801-1846 (2000).

[25] 389 U.S. 347 (1967).

[26] *Id.* at 358 n. 23. *Katz* overruled *Olmstead v. United States*, which held that tapping of wires that did not involve a physical intrusion was not a search and seizure under the Fourth Amendment. Olmstead v. United States, 277 U.S. 438, 466 (1928)

[27] *Katz*, 389 U.S. at 358 n. 23.

[28] Pub.L. 90-351, 82 Stat. 197 (June 19, 1968). Some of the requirements under Title III are more restrictive than what is required under the Fourth Amendment.

[29] 18 U.S.C. §§ 2516(1), (3); 18 U.S.C. § 2518(5), (6), (8)(a).

[30] *Id.* §§ 2518(4), (11).

sary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States," or "limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against any clear and present danger to the structure or existence of the Government."[31] These caveats seemed to suggest that "national security" wiretaps in both domestic and international investigations could continue outside the parameters of Title III. In 1972, however, during the Vietnam War, the Supreme Court held in *United States v. United States District Court (Keith)* that the president had no constitutional power to conduct warrantless surveillance of domestic individuals and organizations that have "no significant connection" to a foreign power.[32] In *Keith*, the defendants were accused of trying to bomb a CIA office in Ann Arbor, Michigan, but there was no connection to a foreign power or entity. The Supreme Court held that surveillance of domestic targets – even under circumstances of "clear and present" danger – is unconstitutional without a judicial warrant based on probable cause, and meeting the particularity requirements of the Fourth Amendment.[33] Nonetheless, the Supreme Court left open the possibility that the president may have authority to conduct warrantless surveillance of foreign powers and their agents.[34] (This understanding was the primary basis for President Bush's ordering NSA to conduct warrantless wiretapping post 9/11.[35]) Significantly, after *Keith*, every federal appeals court to address the issue, including the FISCR, has concluded that the president has the inherent authority to conduct warrantless surveillance to gather foreign intelligence.[36]

Although *Keith* held that a warrant is required to conduct surveillance of domestic security threats, the Supreme Court did note that the issuance of a warrant for intelligence purposes "may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."[37] The Court intimated that Congress could create warrant requirements that would be "more appropriate to domestic security cases" and that did not have to follow the strict requirements of Title III. Interestingly, the Court even mentioned that a "specially designated court" could be used.[38]

---

[31] *Id.* § 2511(3).

[32] United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 309 (1972).

[33] *Id.* at 314-16.

[34] *Id.* at 321-22.

[35] *See infra* Part II where this Article discusses the Terrorist Surveillance Program.

[36] *See , e.g.,* United States v. Truong Dinh Hung, 629 F.2d 908, 913- 14 (4th Cir. 1980); United States v. Butenko , 494 F.2d 593, 603 (3rd Cir. 1974), *In re Sealed Case,* 310 F.3d. at 742, United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977), United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973). It should be noted, however, that except for *In re Sealed Case,* the other cases concerned surveillance occurring before the enactment of FISA.

[37] *Keith*, 407 U.S. at 323.

[38] *Id.*

C. *Foreign Intelligence Surveillance Act of 1978*

In 1978, Congress enacted FISA to deal with the unresolved issue of gathering foreign intelligence (solely domestic intelligence is still governed by Title III). For decades, presidents had conducted electronic surveillance for national security purposes without a warrant. Indeed, wiretaps for such purposes were authorized by presidents at least since the administration of Franklin Roosevelt in 1940.[39] In the 1960s, Presidents Johnson and Nixon used the agency to listen in on hundreds of Americans, including Vietnam War protesters and the Rev. Martin Luther King Jr.[40] During the Watergate scandal in the 1970s, President Nixon relied on national security concerns to hide his wiretapping of domestic political opponents.[41] Between 1975-1976, the Church Committee did an exhaustive inquiry into domestic spying and discovered (1) that the FBI had conducted 500,000 investigations into alleged subversives from 1960-1974; (2) that the CIA had engaged in widespread mail-openings in the United States; (3) that Army intelligence operatives had conducted secret inquiries against 100,000 U.S. citizens opposed to the Vietnam War; (4) that the NSA monitored every cable sent overseas or received by Americans from 1947 to 1975; and (5) that the NSA conducted surveillance of telephone conversations of an additional 1680 citizens.[42] All these aforementioned acts were taken with no judicial oversight.

As a result of these governmental abuses of civil liberties, and as a result of the *Keith* decision that suggested that the rules for gathering intelligence may be different than the rules for law enforcement, in 1978 Congress enacted FISA to replace presidentially ordered surveillance of national security threats and to reign in politically motivated surveillance.[43] FISA provides a statutory framework for the U.S. government to engage in electronic surveillance and physical searches[44] to obtain "foreign intelligence information," which generally encom-

---

[39] *See, e.g.*, United States v. United States District Court, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson); Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program*, 60 STAN. L. REV. 1023, 1025 (February 2008).

[40] Maria Godoy, *The NSA: America's Eavesdropper-in-Chief*, NPR.ORG, Feb. 3, 2006.

[41] For statistics on the amount of intelligence gathered on Americans between 1947 and 1975, *see* Williams C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1226-1227 (May 2007).

[42] Loch K. Johnson, *NSA Spying Erodes Rule of Law, in* INTELLIGENCE AND NATIONAL SECURITY, THE SECRET WORLD OF SPIES 411 (Loch K. Johnson and James Wirtz, eds., 2008).

[43] *See generally* BANKS, *supra* note 41, at 1211.

[44] As enacted in 1978, FISA covered only electronic surveillance. It was amended in 1994 to cover physical searches and again in 1998 to cover pen register, trap and trace devices, and business records acquisition. *See* 50 U.S.C. § 1821 *et seq.* (physical searches), § 1841 *et seq.* (pen register, trap and trace devices, and business records).

passes evidence of terrorism, espionage, and sabotage.[45] Like Title III, FISA surveillance can target U.S. citizens as well as foreign nationals inside this country, but provides simplified procedures for obtaining and executing warrants for both electronic surveillance and physical searches. FISA allows wiretapping of aliens and citizens in the U.S. based on a finding of probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power.[46] Significantly, unlike Title III which requires a finding of probable cause that the search will reveal evidence of a crime, under FISA the government only needs to establish probable cause that the target is a member of a foreign terrorist group or an agent of a foreign power. This lower threshold for conducting surveillance under FISA reflects the inherent differences between obtaining surveillance for intelligence (e.g. prevention) purposes, as opposed to obtaining evidence to be used to convict an individual in a court of law. Although the Supreme Court has not ruled on the constitutionality of FISA, several lower courts have upheld its constitutionality even without traditional probable cause, because "governmental interests in gathering foreign intelligence are of paramount importance to national security, and may differ substantially from those presented in the normal criminal investigation."[47]

FISA does provide some added protection for U.S. citizens and permanent resident aliens (referred to as "U.S. persons" in FISA). To obtain a FISA warrant targeting a U.S. person, there must also be probable cause to believe that the person is "knowingly" engaged in activities that "involve or may involve a violation of the criminal statutes of the United States."[48] In other words, while suspicion of illegal activity is not required in the case of aliens who are not permanent residents – as applied to them, membership in a terrorist group or

---

[45] "Foreign intelligence information" is a term of art and is defined as "information related to and, if concerning a United States person, necessary to, the ability of the United States to protect against an actual or potential attack, terrorism or sabotage by a foreign power or agents thereof, or clandestine intelligence activities of a foreign power or agent thereof, or information with respect to a foreign power or foreign territory that relates to and, if concerning a United States person, is necessary to, the national security of the United States or the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e).

[46] 50 U.S.C. § 1805. As of 2004, the government can also target a non-U.S. person who is considered a "lone wolf," meaning a person not necessarily linked to a foreign group *per se* but is planning to engage in international terrorism. §§ 1801(a)-(b), 1805(a)-(b). "Foreign power" is defined broadly to include, *inter alia,* "a group engaged in international terrorism or activities in preparation therefore" and "a foreign-based political organization, not substantially composed of United States persons." §§ 1801(a)(4), (5). The definition of an "agent of a foreign power" includes any person who "knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power[,]" or any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." §§ 1801(b)(2)(A),(c).

[47] United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987).

[48] 50 U.S.C. § 1801(b)(2)(a).

being an agent of a foreign power is enough – for U.S. persons there must be the additional linkage to knowingly engaging in activity that may be a crime. Furthermore, any investigation of a U.S. person may not be conducted solely on the basis of activities protected by the First Amendment to the Constitution.[49]

Applications for FISA warrants go to federal judges that comprise the Foreign Intelligence Surveillance Court (FISC). Like a grand jury proceeding, the FISC conducts its business ex parte, meaning the government is the only party present at its proceedings. Appeals from the FISC go to the FISCR. The FISC has jurisdiction to hear applications for, and to grant court orders approving, electronic surveillance or physical searches anywhere in the United States to obtain foreign intelligence information under FISA.

In order for an executive official to get a FISA warrant to conduct "electronic surveillance," the FISC must approve several requirements: (1) probable cause that the target is an agent of a foreign power or a foreign power (and the additional requirements discussed above if the target is a U.S. person);[50] (2) probable cause that the target is using or about to use the "facility" to be monitored;[51] (3) applicable "minimization procedures" designed to minimize the acquisition and retention, and to prevent the dissemination, of information concerning U.S. persons that is unrelated to foreign-intelligence;[52] (4) a certification that the information sought "cannot reasonably be obtained by normal investigative techniques,"[53] and (5) the Attorney General must approve the application and a high-ranking intelligence official must certify that a "significant purpose" of the surveillance is to gain foreign intelligence information.[54] If the target is a U.S. person, the basis for the aforementioned review is subject to review for clear error.[55]

FISA also has specific provisions for warrantless surveillance, such as allowing for electronic surveillance without a court order for fifteen days following a declaration of war by Congress.[56] Furthermore, the statute allows for emergency wiretaps for seventy-two hours as long as a warrant is prepared

---

[49] *Id.* § 1805.

[50] *Id.* § 1805(a)(2). In making the probable cause determination, the judge may consider past activities of the target as well as facts and circumstances relating to the target's current or future activities. *Id.* § 1805(b).

[51] 50 U.S.C. § 1805(a)(3). Pursuant to the USA Patriot Act, if the government can show that the target is likely to take steps to impede the surveillance, the government can request a roving wiretap that can follow the target if he changes his means of communication. *Id.* § 1805(c)(2)(B).

[52] 50 U.S.C. §§ 1805(a)(3), 1801(h).

[53] *Id.* § 1804(a)(7)(E).

[54] *Id.* § 1805(a)(4).

[55] *Id.* § 1805(a)(4).

[56] *Id.* § 1811.

during that time frame.[57] FISA also allows warrantless surveillance for up to one year for communications "used exclusively between or among foreign powers" where there is "no substantial likelihood" that a communication involving a U.S. person would be acquired.[58]

Significantly, as will be discussed below in more depth, the government does not need a warrant to conduct electronic surveillance overseas. The Supreme Court has not addressed the controversial question as to what extent the executive needs a warrant to conduct surveillance and searches, for intelligence purposes, of domestic targets suspected of international terrorism.[59] As explained previously, conducting domestic surveillance with no connection to a foreign power merits a warrant based on probable cause, but the question is murkier when there is a connection to a foreign power.[60] In August 2008, the FISCR specifically found a foreign intelligence exception to the warrant requirement.[61] While searches involving U.S. persons must still be reasonable under the Fourth Amendment, if the surveillance's "programmatic purpose" is "beyond ordinary crime control," then a warrant is not needed.[62] At this point, it is unknown whether the Supreme Court would agree.

FISA is a complicated statute. The rules change depending on (1) whether the target of the surveillance is a U.S. person or foreign national; (2) whether the target is located in the United States or overseas; (3) whether the acquisition/collection of the intelligence takes place in the United States or overseas; (4) whether the acquisition/collection is conducted by fiber optic cable/wire or wireless communication; and (5) whether the purpose of the surveillance is targeted at a particular individual or whether the acquisition is merely incidental to targeting a different person. In other words, the requirements change depending on who the target is, where he is situated at the time of the surveillance, and how and where the agency/agents acquired the surveillance. In order to appreciate what is really at stake with the FAA of 2008, it is critical that the reader understand how the original FISA operated and what it regulated.

As a fundamental matter, FISA never intended to require a warrant to capture overseas communications between two foreign nationals who do not have Fourth Amendment rights.[63] The complicated question is to what extent FISA

---

[57] *Id.* § 1805(f).

[58] *Id.* §1809(a)(1).

[59] *Keith*, 407 U.S. at 309, n.8; *Katz*, 389 U.S. at 358 n.23 (1967); Mitchell v. Forsyth, 472 U.S. 511, 531 (1985).

[60] *See supra,* Section I.B, discussing the *Keith* case.

[61] *In re Directives * Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, No. 08-01, 15 (FISA Ct. Rev. Aug. 22, 2008).

[62] *Id.*

[63] As the Supreme Court held in United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), only persons who "have come within the territory of the United States and developed substantial connections" to the country have Fourth Amendment rights. *Id.* at 271. In fact, in November 2008, the Second Circuit held that the warrant requirement does not even apply

covers international communications between a foreign national overseas and a U.S. person within the United States. This question is further confounded by a distinction in FISA between wireless communications (such as by radio), which FISA generally does not regulate for international communications, and communications conducted by fiber optic wire or cable, which FISA does regulate if the cable or wire is intercepted within the United States.[64] For instance, if a foreign national overseas is communicating with a person in the United States, and the physical interception is taking place on a wire or cable in the United States, FISA requires a warrant.[65] Yet, if the same communication is intercepted on a wire outside of the United States (such as a transoceanic cable), FISA does not require a warrant so long as the surveillance is not intentionally targeting a person known to be in the U.S. If the same foreign national overseas and U.S. person in the United States are now communicating by wireless communication (such as by radio), FISA also does not require a warrant, even if the interception takes place within the United States, as long as the purpose of the surveillance is not to target a person known to be in the U.S. In other words, FISA seems to make arbitrary distinctions, based on technology, that are divorced from any privacy or reasonableness concerns of the Fourth Amendment.

---

to U.S. citizens in foreign countries, although any searches, including warrantless surveillance, must still be reasonable. *See* In re Terrorist Bombings of U.S. Embassies in East Africa, No. 01-1535-cr (L) (2nd Cir. Nov. 24, 2008). Prior to the FAA, FISA also did not cover the acquisition of communications of U.S. persons overseas, although an executive order required that there be probable cause that the U.S. person overseas was an agent of a foreign power. In other words, when Congress enacted FISA in 1978, its purpose was to regulate the gathering of foreign intelligence *within* the United States.

[64] Before the enactment of the FAA, FISA defined "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any *wire or radio* communication sent by or intended to be received by a particular, *known* United States person who is in the United States, if the contents are acquired by *intentionally targeting* that United States person. . ."; "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any *wire* Communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs *within* the United States . . . ."; "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any *radio* communication . . . *if both the sender and all intended recipients are in the United States*;" or "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication . . ." 50 USC 1801(f)(1)-(4) (Emphasis added). In other words, FISA defines wire communication as "electronic surveillance" if the acquisition takes place in the United States or a U.S. person in the United States is the target while it defines radio communication as "electronic surveillance" only if sender and intended recipients are in the United States or the target is a U.S. person in the United States. As will be explained in Section IV.A, *infra*, the FAA simplifies the definition of "electronic surveillance" by not focusing on the kind of technology being used or where the acquisition takes place.

[65] 50 U.S.C. § 1801(f)(1)– (2).

As Michael McConnell, former Director of National Intelligence (DNI), explained to the Senate Judiciary Committee in September 2007, when Congress enacted FISA in 1978 it was not supposed to regulate international communications between a foreign national overseas and a U.S. person in the United States as long as the *intent* was to target the person overseas.[66] In 1978, most international communications took place wirelessly and not through fiber optic cable; therefore, even if the acquisition took place within the United States, the acquisition would not be covered by FISA.[67]

D. *U.S.A. Patriot Act*

After 9/11, the Department of Justice worked to expand the surveillance tools needed to gather intelligence on terrorist activity. Approximately five weeks after 9/11, Congress passed the U.S.A. Patriot Act,[68] which, *inter alia,* increased emergency surveillance before obtaining a FISA warrant from twenty-four hours to seventy-two hours,[69] expanded the number of FISA judges from seven to eleven,[70] expanded the availability of physical searches, pen registers, and trap and trace devices,[71] and allowed roving wiretaps.[72] It also extended the time periods for the surveillance from 90 days to 120 days.[73] While a thorough analysis of the Patriot Act is beyond the scope of this Article, for purposes of the later discussion in Part IV (analyzing the FAA), it is useful to discuss (arguably) the most consequential change to FISA: the requirement that a "significant purpose" as opposed to "the purpose" of the surveillance be to conduct foreign intelligence.

Before 9/11, to obtain a FISA warrant, the government had to assert that the "purpose of the surveillance is to obtain foreign intelligence information."[74] Over the years, based on several court decisions, the government interpreted "purpose" to be "primary purpose" to gain foreign intelligence information.[75]

---

[66] *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing on FISA and Implementation of the PAA, Before S. Judiciary Comm.* 110th Cong. 4 (2007) [hereinafter *Strengthening FISA Hearings*] (statement of Michael McConnell, Director of National Intelligence). *Available at* http://www.fas.org/irp/congress/2007_hr/092507mcconnell.pdf.

[67] *Id.* at 6.

[68] Pub.L. No. 107-56, § 208(1), 115 Stat. 283 (2001).

[69] *Id.* § 208(1), 115 Stat. 283 (2001)

[70] *Id.*

[71] *Id.* § 214, 115 Stat. at 286.

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

[73] *Id.* § 207(a), 115 Stat, at 282.

[74] 50 U.S.C. § 1804(a)(7)(B) (2000).

[75] United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Duggan, 743 F.2d 59, 7778 (2d Cir. 1984), United States v. Pelton, 835 F.2d 1067, 1075-

Furthermore, a 1995 Office of Legal Counsel (OLC) opinion concluded that "courts are more likely to adopt the 'primary purpose' test than any less stringent formulation," and that "the greater the involvement of prosecutors in the planning and execution of FISA searches, the greater is the chance that the government could not assert in good faith that the 'primary purpose' was the collection of foreign intelligence."[76] If evidence of criminal wrongdoing was discovered pursuant to a properly executed FISA warrant (where the primary purpose was to collect intelligence), this evidence could still be used at trial.[77] Nonetheless, because of fears that zealous prosecutors would manipulate FISA warrants to bypass the need to obtain traditional law enforcement warrants under Title III (with the more rigorous probable cause standard), a "wall" was created that impeded prosecutors from discussing their cases with intelligence officers or controlling, initiating, or expanding FISA investigations. In fact, "in 1995, the Reno Justice Department issued guidelines that FISA information could almost never be shared with criminal investigators."[78] It is this artificial wall – one created by custom, bureaucracy, and practice but not by law – that the 9/11 commissioners criticized in the 9/11 Commission Report.[79] As law professor William Banks attests, the "FISA wall procedures were designed to protect against using the secretive foreign intelligence collection process in order to build a criminal case," but "never stood in the way of the sharing of criminal information with intelligence investigators," nor "the sharing of intelligence information with criminal investigators, so long as the sharing met the foreign intelligence purpose rule."[80]

The Patriot Act changed the legal standard for a FISA warrant from one whose "primary purpose" was to gather foreign intelligence to one that only needed a "significant purpose." Some individuals, like law professor Stephen Schulhofer at New York University, argue that adding the word "significant"

---

76 (4th Cir. 1987), United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987), United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991).

[76] BANKS, *supra* note 41, at 1236-37 (quoting *Implementation of the USA PATRIOT ACT: Section 218 – Foreign Intelligence Information ("The Wall"): Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 17-34 (2005) (statement of David S. Kris, Senior Vice President, Time Warner Inc.)).

[77] *See e.g., Pelton*, 835 F.2d at 1076 (holding that the evidence gathered was admissible because the primary purpose for collecting it was to gather foreign intelligence information); *Duggan*, 743 F.2d at 78 (holding 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 evidence in a criminal trial.")

[78] JOHN YOO, WAR BY OTHER MEANS, AN INSIDER'S ACCOUNT OF THE WAR ON TERROR 81 (2006). For a thorough recounting of the artificial wall that was created, see BANKS, *supra* note 41, at 1236-39.

[79] THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 537-38 n. 71, 539 n.83 (2004).

[80] BANKS, *supra* note 41, at 1265.

produces a "large change in law enforcement power."[81] According to Schulhofer, the change to the phrase "significant purpose" from "purpose" means that U.S. citizens and foreign nationals may be exposed to "broad FISA surveillance" when the government's primary purpose is not to gather foreign intelligence but instead to gather evidence for use at a criminal trial.[82] Similarly, Banks argues in *The Death of FISA* that the change to "significant purpose" essentially "gutted the central premise of FISA" because it allows "the primary objective of the planned surveillance [to be] evidence to support a prosecution."[83] Banks observes that, since 9/11, there has been a "growing criminalization of terrorism-related activities [that] has made the prosecutorial agenda a larger part of the sphere of electronic surveillance and has accordingly further complicated the task of managing FISA implementation."[84]

Nonetheless, in 2002, the FISCR specifically upheld the change to "significant purpose" as lawful, despite the overlap between intelligence and criminalization of terrorist activities. As the FISCR explained:

> [The primary purpose] analysis, in our view, rested on a false premise and the line the court sought to draw was inherently unstable, unrealistic, and confusing. The false premise was the assertion that once the government moves to criminal prosecution, its 'foreign policy concerns' recede. . . . [T]hat is simply not true as it relates to counterintelligence. In that field the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts.[85]

In other words, criminal prosecution and the gathering of foreign intelligence are often intertwined, and one way to prevent threats to national security is to prosecute terrorists. Furthermore, the FISCR aptly noted that the definition of an agent of a foreign power for U.S. persons is rooted in criminal conduct (i.e. knowingly engaging in activity that may be a crime).[86] The FISCR concluded that unless the government's "sole objective" was to obtain evidence of a past crime, a FISA warrant should be granted.[87] The FISCR stressed, however, that the "FISA process may not be used to investigate wholly unrelated ordinary crimes."[88] While the Supreme Court has yet to rule on the constitutionality of FISA or the specific change to "significant purpose," all other courts to consider the issue, except one district court, have agreed with the FISCR's holding that the change to "significant purpose" is reasonable under the Fourth Amend-

---

[81] STEPHEN SCHULHOFER, THE ENEMY WITHIN 44 (2002).

[82] *Id.* at 44-45.

[83] BANKS, *supra* note 41, at 1213.

[84] *Id.* at 1214.

[85] In re Sealed Case, 310 F.3d 717, 743 (FISA Ct. 2002).

[86] *Id.* at 723.

[87] *Id.* at 735-36.

[88] *Id.*

ment.[89]

In sum, after September 11, it was assumed that the Bush administration was operating under FISA as amended by the Patriot Act. If there were concerns that FISA was inadequate to meet the terrorist threat, those concerns were neither expressed to the intelligence committees of Congress nor the American public. The next section of this Article analyzes the Bush administration's warrantless wiretapping program (i.e. the TSP) and to what extent it violated the Constitution and FISA. As will be explained, an outgrowth of the TSP was the enactment of the FAA in July 2008. In order to appreciate the nuances of the FAA, it is incumbent to understand the underlying rationale of the TSP, even if the reader concludes that the TSP was unlawful.

II. NSA WIRETAPPING

A. *Background*

The National Security Agency (NSA) intercepts and decodes communications around the world to protect the United States from foreign security threats. As explained previously, the NSA can legally conduct wiretapping outside the United States with no need for a warrant. After September 11, the Bush administration directed the NSA to intercept the substance of electronic communications that started or ended in the United States, if one person was believed to be linked to al Qaeda. Normally, as explained previously, the NSA would need to obtain a FISA warrant to conduct surveillance in the United States if the target was a U.S. person.[90] Yet, the Bush administration decided that it was too cumbersome to obtain FISA warrants when time was of the essence in detecting terrorist plots and maintained that it had the legal authority under Article II of the Constitution, and Congress's passing of the Authorization for Use of Military Force (AUMF)[91] (discussed subsequently), to bypass

---

[89] Every court to consider the constitutionality of FISA, with the exception of the court in Mayfield v. United States, 504 F.Supp.2d 1023 (D. Or. 2007), has found FISA to comply with the Fourth Amendment. *See e.g.*, United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005); In re Grand Jury Proceedings, 347 F.3d 197, 206 (7th Cir. 2003); United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir.1987); United States v. Jayyousi, No. 0460001CR (Cooke), 2007 WL 851278, at *1 (S.D. Fla. Mar. 15, 2007); United States v. Benkahla, 437 F.Supp.2d 541, 555 (E.D.Va.2006); United States v. Marzook, 435 F.Supp.2d 778, 786 (N.D. Ill. 2006); United States v. Sattar, No. 02CR395 (JGK), 2003 WL 22137012, at *13*15 (S.D.N.Y. Sept. 15, 2003); Global Relief Found., Inc. v. O'Neill, 207 F.Supp.2d 779, 807 (N.D. Ill. 2002); United States v. Nicholson, 955 F.Supp. 588, 590 n. 3 (E.D. Va.1997) (collecting cases); United States v. Mubayyid, 521 F.Supp.2d 125, 139-40 (D. Mass. 2007) (holding change to "significant purpose" to be constitutional on its face).

[90] *See supra* Section I.B. discussing *Katz* and *Keith* cases.

[91] Authorization for Use of Military Force, Pub. L. 107-40, §2(a), 115 Stat. 224, (2001).

the FISA statute.[92]

The *New York Times* disclosed the existence of this secret NSA program in December 2005 and the administration admitted that the program existed but refused to reveal the full extent of the program.[93] Former Attorney General Alberto Gonzales stated in a December 2005 press release that "the program remains highly classified; there are many operational aspects of the program that have still not been disclosed and we want to protect that because those aspects of the program are very, very important to protect the national security of this country."[94] Nonetheless, Gonzales did describe some of its parameters, telling reporters that it involves "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[95]

It is undisputed that the NSA bypassed the FISA court and conducted surveillance on domestic communications without a warrant. The pivotal issue is to what extent the NSA has the legal authority to eavesdrop inside the country without following FISA. Many prominent jurists,[96] as well as the Congressional Research Service,[97] a non-partisan arm of Congress, concluded that the NSA wiretapping program was illegal as it violated the Fourth Amendment and FISA, which they argue is the exclusive statute monitoring foreign surveillance. Conversely, the Bush administration asserted that the NSA wiretapping was lawful based on the president's inherent authority as Commander in Chief under Article II of the Constitution, and Congress's passing of the AUMF after September 11 allowing the president to "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001."[98]

B. *Legal Arguments*

The legal issues surrounding the NSA wiretapping program are complex, implicating constitutional law, statutory law, canons of constitutional interpre-

---

[92] *See infra* Section II.B. discussing the Bush administration's rationale for the warrantless wiretapping program,

[93] RISEN & LICHTBLAU, *supra* note 3.

[94] Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, the White House (Dec. 19, 2005) [hereinafter "Press Briefing"] *Available at http://www.globalsecurity.org/intell/library/news/2005/intell-051219-dni01.htm.*

[95] *Id.*

[96] Several law professors wrote an open letter to Congress explaining how the TSP was unconstitutional and violated FISA. *See* DAVID COLE, JUSTICE AT WAR 131-45 (2008).

[97] BAZAN & ELSEA, *supra* note 5.

[98] Authorization for Use of Military Force § 2(a).

tation, and national security law. The purpose of this section is to highlight the main legal issues. This section in no way, however, exhausts all the relevant legal issues.

Critics argue that FISA provides the exclusive manner to conduct foreign surveillance; therefore it was unlawful for President Bush to bypass its provisions by executive order. These critics also emphasize that FISA already contains provisions for warrantless surveillance such as allowing emergency wiretaps without a warrant for seventy-two hours as long as a warrant is obtained within that time frame; or allowing warrantless surveillance fifteen days following a declaration of war by the Congress; or allowing the Attorney General to conduct warrantless surveillance for up to one year if U.S. persons are not the targets.[99] Hence, critics contend that, given the exceptions for warrantless surveillance, there was no need for the President to bypass the statutory scheme created by Congress.[100] Furthermore, critics maintain that Congress had been willing to amend FISA as it did with the Patriot Act, so there was no justification for the executive to unilaterally bypass FISA without Congressional authorization.[101]

The Bush administration countered that FISA was not exhaustive and allowed for subsequent statutes concerning foreign surveillance. Specifically, FISA prohibits any person from intentionally "engaging . . . in electronic surveillance under color of law *except as authorized by statute*."[102] Therefore, the Bush administration maintained that in enacting FISA, Congress contemplated the possibility that the president might be permitted to conduct electronic surveillance pursuant to a later-enacted statute that did not incorporate all of the procedural requirements set forth in FISA, or that did not expressly amend FISA itself.[103] Furthermore, the Bush administration claimed that the AUMF passed by Congress on September 14, 2001 (which authorizes the president "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001") qualified as such a statute, authorizing electronic surveillance within the meaning of FISA.[104] According to the Bush administration, the broad language of the AUMF afforded the presi-

---

[99] *See* 50 U.S.C. § 1805(f) (2)(2000) (emergency wiretaps for seventy-two hours); *Id.* § 1811 (2000) (electronic surveillance without a court order for fifteen days following a declaration of war); *Id.* § 1802 (a)(1)(2000) (Attorney General to order electronic surveillance without a court order for up to one year for non US persons to acquire foreign intelligence information).

[100] BAZAN & ELSEA, *supra* note 5, at 27.

[101] COLE, *supra* note 5, at 19.

[102] 50 U.S.C. § 109(a)(1) (emphasis added).

[103] Memorandum from the U.S. Department of Justice, "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," 20-21, (Jan. 19, 2006).

[104] PRESS BRIEFING, *supra* note 94.

dent, at a minimum, discretion to employ the traditional incidents of the use of military force, which included surveillance.[105] The Bush administration pondered how it could use "force" if it could not first locate the targets, which obviously required surveillance. The Bush administration further supported a broad reading of the AUMF by citing to the Supreme Court's decision in the case of *Hamdi v. Rumsfeld*,[106] where the Court held that the AUMF implicitly authorized the president to detain enemy combatants, even though the AUMF contained no explicit mention of that power.[107]

Critics responded that the general provisions of the AUMF allowing the executive to use "necessary force" did not supersede the specific and detailed provisions of FISA.[108] Furthermore, they attested that *Hamdi* concerned whether the Bush administration could detain an individual caught in the middle of a battlefield as an enemy combatant, and had nothing to do with surveillance.[109] Critics further asserted that it is not clear that the collection of intelligence constitutes a use of "force" as authorized under the AUMF.[110]

C. *Analysis*

Professor and former Assistant Attorney General Jack Goldsmith wrote in *The Terror Presidency* that President Bush and Vice President Cheney "wanted to leave the presidency stronger than they found it."[111] He observed, however, that "they seemed to have achieved the opposite. They *borrowed against the power of future presidencies* – presidencies that . . . will be viewed by Congress and the courts, whose assistance they need, *with a harmful suspicion and mistrust because of the unnecessary unilateralism of the Bush years.*"[112] The problem with the TSP was not so much in what it did, but how the Bush administration went about doing it. By initiating a secret program that bypassed Congress, the Bush administration sacrificed trust for assumed security when it could have simultaneously increased both. There is no evidence that Congress, which amended FISA with the Patriot Act five weeks after 9/11, and later enacted the Protect America Act and the FAA, would have balked at FISA reform had the TSP been proposed and debated initially.

Whether the TSP was unconstitutional remains undecided, but it probably did violate FISA. As discussed in Part I, the Supreme Court has not yet decid-

---

[105] *Id.*

[106] Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (plurality).

[107] *Id.*; *see also* PRESS BRIEFING, *supra* note 94. While the Hamdi decision only garnered four votes, Justice Thomas joined the plurality for the point that the AUMF authorized the president to detain enemy combatants.

[108] BAZAN & ELSEA, *supra* note 5, at 3.

[109] *Id.* at 34-35.

[110] *Id.* at 35. For a succinct review of the arguments that the TSP was unlawful, *see* Cole, *supra* note 5.

[111] JACK GOLDSMITH, THE TERROR PRESIDENCY 140 (2007).

[112] *Id.* (emphasis added).

ed whether it is unconstitutional for the executive to conduct warrantless surveillance on agents of foreign powers or international terrorist groups within the United States, as opposed to spying on purely domestic groups, which would require a warrant per *Keith*.[113] Appellate courts and the FISCR have held that the president does indeed have constitutional power to conduct warrantless surveillance for national security purposes as long as the target has a connection overseas.[114]

Although the TSP may be illegal under FISA, and despite the compelling arguments made by the TSP's critics, it is far from clear that the NSA wiretapping program violated the Fourth Amendment. There are many situations where warrants are not required before a search commences.[115] While the search must still be reasonable under the circumstances, given that the purpose of the TSP was to obtain foreign intelligence for national security purposes—and not to obtain evidence of ordinary crime—and given that the TSP (at least based on the information disclosed) only targeted communications with suspected al Qaeda operatives, the TSP likely does not violate the Fourth Amendment (especially since presidents have been conducting warrantless surveillance for national security purposes since at least 1940).[116]

Concededly, the TSP most likely violated a law passed by Congress – FISA. While Article II of the Constitution makes the President the Commander in Chief,[117] Article I of the Constitution provides that Congress shall ratify treaties, declare war, fund and regulate military forces and make laws "necessary and proper" for the execution of all presidential powers.[118] However, the Constitution does not mention "surveillance" or "spying," which leaves ambiguous which branch of the government controls the power to authorize and regulate those activities. Although presidents conducted warrantless surveillance for national security purposes before Congress enacted FISA in 1978,[119] Congress created FISA in part to reign in and halt the abuses that had occurred in the 1960s and 1970s when the FBI and NSA spied on U.S. citizens for political reasons.[120] In Justice Robert Jackson's concurring opinion in *Youngstown Sheet and Tube Co. v. Sawyer*, he laid out the lowest ebb of Presidential power: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over

---

[113] *Keith, supra* note 32.u

[114] *See* note 36, *supra.*

[115] *See* notes 8-18, *supra.*

[116] *See* note 39, *supra.*

[117] U.S. CONST. art. II.

[118] U.S. CONST. art. I.

[119] *See* notes 39-42, *supra.*

[120] *See* note 42, *supra.*

the matter."[121] Even under the best of circumstances, President Bush was at his "lowest ebb of power" because Congress had specifically enacted legislation addressing surveillance. Given that FISA contains exceptions for warrantless surveillance, and that Congress was amenable to amending FISA post 9/11 with the Patriot Act, the more prudent approach would have been for the president to seek additional FISA amendments, or request a new statute broadening the executive's powers to conduct surveillance, rather than unilaterally bypassing the Congressional (and thus legislative) scheme in favor of using the secretive TSP.

Furthermore, the Bush administration's argument that the AUMF provided Congressional authorization for warrantless surveillance by bypassing the specific provisions of FISA[122] appears to be overreaching, especially given that Congress had just amended FISA with the Patriot Act at the same time that it issued the AUMF. As the *Washington Post* observed: "Clearheaded members of Congress voting for the [AUMF] certainly understood themselves to be authorizing the capture of al Qaeda and Taliban fighters. We doubt any members even dreamed they were changing domestic wiretapping rules – particularly because they were focused on that very issue in passing the USA Patriot Act."[123] Furthermore, the Bush administration's broad interpretation of the AUMF means that the executive can unilaterally make any decision affecting any aspect of the war on terror with impunity and no oversight by Congress, whether that decision is detaining U.S. citizens indefinitely as enemy combatants or spying on U.S. citizens without a warrant. As CATO Senior Fellow Robert Levy testified before Congress, if warrantless surveillance is part of the president's inherent wartime powers, then what about sneak-and-peak searches, roving wiretaps, library record searches, and national security letters – all of which were debated and reauthorized in the Patriot Act.[124] If the president has inherent wartime powers that allow him to secretly bypass or ignore explicit legislation enacted by Congress, the implications are staggering. A fair reading of the AUMF does not support such an expansion of executive power.[125]

The Bush administration argued that it could not use force against al Qaeda if it did not know where al Qaeda was situated.[126] But, FISA does provide the

---

[121] Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J. concurring).

[122] *See* PRESS BRIEFING, *supra* note 94.

[123] Editorial, *The Power to Spy*, WASH. POST, Dec. 25, 2005, at B06.

[124] *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings on NSA Before the S. Comm. on the Judiciary*, 109th Cong. 7 (2006) [hereinafter *NSA Hearings*] (statement of Robert A. Levy, Senior Fellow in Constitutional Studies, Cato Inst.).

[125] The AUMF authorizes the President to "to use all necessary and appropriate force against those nations, organizations or persons" who "planned, authorized, committed or aided" the 9/11 attacks. Pub. L. 107-40, 115 Stat. 224 (2001).

[126] *See* PRESS BRIEFING, *supra* note 94.

executive with tools for surveillance, including warrantless surveillance,[127] and if the president found FISA's tools inadequate, he could have asked Congress for new authority. Hence, while it is arguable whether President Bush actually broke the law with his secret NSA wiretapping program, it certainly was an unwise policy decision that cost him political capital, enormous criticism, undermined his credibility, and served as a huge distraction to his administration.[128] As of January 2007 (mainly due to pressure from telecommunications companies that were being sued),[129] the Bush administration began to subject the TSP to the scrutiny of the FISA court.[130]

While it is easy and justifiable to condemn the Bush administration for the way it initiated the TSP, a responsible analysis must address why, to achieve its surveillance goals, the Bush administration felt it needed to bypass Congress and the FISA court, especially when Congress was simultaneously amenable to amending FISA with the Patriot Act.

III: FISA'S ADEQUACY IN THE WAR ON TERROR.

To what extent can FISA, created during the Cold War, protect U.S. national security interests in a world of transnational terrorism where the government may not have "probable cause" that individuals are connected with a foreign power or international terrorism? According to former Deputy Director of Na-

---

[127] *See* note 99, *supra.*

[128] *See, e.g.*, RISEN & LICHTBLAU, *supra* note 3.

[129] Hepting v. AT & T, No. C-06-0627-JCS (N.D. Cal. Filed Jan. 31, 2006) (class action lawsuit filed by Electronic Frontier Foundation against AT & T and other telecommunications providers for participating in the NSA surveillance program). In July 2008, the FAA, discussed *infra* at Section IV.A, granted retroactive immunity to the telecommunication providers if they can demonstrate that they acted in good faith reliance on legal advice provided by the Bush administration. The Electronic Frontier Foundation argues, however, that the immunity provision of the FAA is unconstitutional. This case is currently pending before Judge Vaughn Walker at the U.S. District Court of the Northern District of California. *See* Hepting v. AT & T, 539 F.3d 1157 (9th Cir. 2008) (remanding case to district court in light of FAA).

[130] James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1, *available at* http://www.nytimes.com/2007/08/06/washington/06nsa.html?_r=1&ref=washingto&oref=slogin. Furthermore, in January 2007, the administration was able to convince one of the FISA judges that a warrant was not needed for foreign-to-foreign communications that happened to be routed through a wire or cable in the United States. As such, the Bush administration stated that it was abandoning the TSP. *See* Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 2007), *available* at http://fas.org/irp///agency/doj/fisa/ag011707.pdf. Yet, a few months later, a different FISA judge had a different interpretation of FISA and ruled that a warrant was needed for interceptions occurring on wire or cable in the United States. This decision spurred surveillance reform, which resulted in the Protect America Act and ultimately the FAA.

tional Intelligence, General Michael Hayden, who was the NSA leader during the TSP, "[the TSP was] successful in detecting and preventing attacks inside the United States."[131] The question then becomes why FISA, as amended by the Patriot Act, was not a sufficient tool to stop terrorist attacks? Why did the Bush administration feel that it needed a warrantless surveillance program that targeted Americans' international communications with alleged al Qaeda operatives?

Between 1978 and September 11, 2001, attorney generals issued forty-seven emergency authorizations under FISA.[132] In the first eighteen months after 9/11, the attorney general issued more than 170 emergency authorizations.[133] Furthermore, the FISC rejected and modified more FISA warrants in 2003 and 2004 than even before in its history. The FISA "judges modified 179 of the 5645 requests for court-ordered surveillance and rejected or deferred at least six [warrant requests] – the first outright rejections in the court's history" during the Bush administration.[134] This history supports the proposition that complying with FISA caused some perceived obstacles for the Bush administration. Or, perhaps, FISA was operating effectively and reigning in, albeit marginally (the number of requests modified still shows much deference to the executive), improper surveillance requests. Regardless, no matter how one interprets the data, it is clear that the Bush administration *felt* that FISA was insufficient to meet the terrorist threat. To what extent did the administration's fears justify the secret way it went about handling the matter?

Perhaps the Bush administration felt it needed to bypass FISA because it did not have probable cause that the targets it sought were agents of foreign powers, or believed it did have probable cause but felt it did not have adequate time to comply with seeking a FISA warrant.[135] In other words, the rationale for the TSP may have been based on a belief that the substantive probable cause standard was too demanding, or the TSP was preferred in order to simply bypass the procedural requirements of FISA in seeking a warrant. The reality may be a little of both. Although Gonzales stated in 2005 that the TSP required the Bush administration have a "reasonable basis" for believing that one party to the call was a terrorist,[136] it is unresolved whether "reasonable basis" was closer to the predicate "probable cause" required by FISA or the lesser standard of "reasonable suspicion."[137] The administration has argued both positions.

---

[131] PRESS BRIEFING, *supra* note 94.

[132] BANKS, *supra* note 41, at 1280.

[133] *Id.*

[134] JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA, 113 (New York, Doubleday 2008).

[135] JOHN CARY SIMS, *What NSA is Doing . . . and Why It's Illegal*, 33 HASTINGS CONST. L.Q. 105, 126-27 (2005-06).

[136] PRESS BRIEFING, *supra* note 94.

[137] *See* Alabama v. White, 496 U.S. 322, 330 (1990) ("Reasonable suspicion is a less demanding standard than probable cause not only in the sense that reasonable suspicion can

While Gonzales stated that "reasonable basis" was essentially the same as "probable cause" under the Fourth Amendment,[138] reports indicate that General Hayden stated that the Bush administration had adopted a "reasonable suspicion" standard in applying the TSP because the probable cause standard in FISA was "too onerous."[139] Complicating matters more, in 2002, a senator tried to change the "probable cause" standard to "reasonable suspicion" for non-US persons under FISA, but the Justice Department did not support the change, arguing that the probable cause standard was not an obstacle to effective use of FISA and that the change to reasonable suspicion would probably be unconstitutional.[140] Such a revelation is especially troubling given General Hayden's statement regarding adopting "reasonable suspicion" as the TSP standard. In essence, it appears that the Bush administration purposefully opted for the lower reasonable suspicion standard with no FISA oversight at all.

Hence, there appear to be two primary rationales for the TSP: (1) that the probable cause standard is too high and (2) that the procedural requirements seeking a FISA warrant are too burdensome. Each potential explanation is addressed in turn.

A. *Substantive Probable Cause Standard*

To what extent is the probable cause standard under FISA sufficient to counter the terrorist threat? As explained previously, unlike Title III, FISA does not require probable cause that a crime is being, has been, or is about to occur before the issuance of a warrant, but rather probable cause that the target is an agent of a foreign power or terrorist group (and for U.S. persons, the additional requirement that the U.S. person may be engaging in activities that knowingly could be a crime).[141] Despite the lower burden under FISA, several policy makers and lawyers argue that requiring probable cause that the target is an agent of a foreign power is too onerous and does not appreciate the complexities in detecting terrorist activity. According to former Deputy Attorney General John Yoo, because FISA "assumes that the government already has [probable cause] to believe that a target is the agent of the foreign power before it even asks for a warrant," FISA works well when the foreign agents are easy

---

be established with information that is different in quantity or content than that required to establish probable cause, but also in the sense that reasonable suspicion can arise from information that is less reliable than that required to show probable cause.")

[138] Alberto R. Gonzales, U.S. Attorney Gen., Dep't of Justice, Prepared Remarks for Attorney General Alberto Gonzales at the Georgetown University Law Center (Jan. 24, 2006), *available at* www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html.

[139] BANKS, *supra* note 41, at 1256 (citing Posting of Glenn Greenwald, GGreenwald@salon.com, to Glenngreenwald.blogspot.com, Unclaimed Territory, *The Administration's New FISA Defense is Factually False*, (Jan. 24, 2006), *available at* www.glenngreenwald.blogspot.com/2006/02/administartions-new-fisa-defeinse-is.html).

[140] BANKS, *supra* note 41, at 1256.

[141] *See supra* Part I.C discussing FISA warrant requirements.

to detect like "foreign embassy, officials working for a hostile nation," or "a Soviet KGB agent operating undercover as a diplomat."[142] Al Qaeda poses a different challenge, however; its members do not work for embassies and are not part of any one nation. Yoo's claims are also supported by former federal prosecutor Andrew McCarthy,[143] and Seventh Circuit appellate judge Richard Posner.[144] As McCarthy explains, "To have probable-cause on a target is to know already that he is dangerous. That's too late. Today's challenge is to discover the unknown Mohamed Atta in our midst, something that can't be done unless surveillance begins whenever it is reasonable to suspect a foreign operative."[145] As Yoo describes, "counterterrorism agencies must search for clues among millions of potentially innocent connections, communications, and links."[146] Judge Posner observes that innocent people may not even be aware that they know or are abetting a terrorist: "[t]he intelligence services must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented."[147] Hence, according to Yoo, McCarthy, and Posner, U.S. intelligence agents need to be able to follow leads quickly and must act fast on educated guesses.

Consider the following example, which is informed by Yoo's description of intelligence gathering in *War By Other Means*:[148] an al Qaeda leader is captured in Europe and his laptop or cell phone has ten U.S. phone numbers on it. It is questionable whether a FISA judge would find probable cause that the users of the ten phone numbers are terrorists.[149] Perhaps, the captured terrorist had called a hotel in the United States to merely make a reservation. Nonetheless, intelligence officials would want to conduct surveillance on the ten individuals—many who may be innocent and not even aware that their communications may have intelligence value—to determine if any are terrorists.[150] As Cato Senior Fellow Robert Levy explains, there may be a need to conduct sur-

---

[142] YOO, *supra* note 78, at 104-05.

[143] Andrew McCarthy, *FISA Reform Debacle in the Making?*, HUMAN EVENTS, Dec. 3, 2007, http://www.humanevents.com/article.php?id=23744#continueA.

[144] *See* RICHARD POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 92-94 (New York: Oxford University Press 2006) (explaining the limitations of FISA when the government needs a warrant to determine whether a person is in fact a terrorist).

[145] MCCARTHY, *supra* note 143.

[146] YOO, *supra* note 78, at 105.

[147] Richard Posner, *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16.

[148] YOO, *supra* note 78, at 106.

[149] *Id.* A similar example is proposed by Judge Posner. *See* Posner, *supra* note 144, at 94.

[150] *See* POSNER, *supra* note 144, at 94 (arguing that when U.S. phone numbers are found on a terrorist, "it would be prudent" to tap all calls to or from those numbers in search of suspicious content, even though most people with these phone numbers are unlikely terrorists themselves).

veillance on individuals who have had "contact" (even innocent contact) with al- Qaeda members, even though these people are not "agents" of a foreign power as FISA currently requires.[151] Yet, as Posner notes: "The government can't get a FISA warrant just to find out whether someone *is* a terrorist; it has to already have a reason to believe he's one."[152] According to Yoo, even if the phone numbers on the cell phone established probable cause, obtaining a FISA warrant is a cumbersome process in which "FBI and DOJ lawyers prepare an extensive package of facts and law to present to the FISA court."[153] The attorney general must also sign off on the application and another national security officer "must certify that the information sought is for foreign intelligence."[154] Yoo maintains that "leads could go stale" during this time period.[155] Yoo concludes that FISA does "not meet today's challenge—a sophisticated, covert, foreign enemy that does not operate out of embassies like the spies of the Cold War, but instead conceals its communications within the billions of innocent phone calls and e-mails sent every day."[156]

General Hayden has expressed the same concern about leads going stale under a rationale of "hot pursuit," where it is felt there is not enough time to obtain a FISA warrant without jeopardizing the surveillance.[157] For instance, if NSA were spying on a terrorist in Yemen and the terrorist called a person in the United States, then NSA could legally listen to the call without a warrant because the target was the Yemeni terrorist. But as soon as the call was complete, NSA could not continue listening to this American's conversations without a FISA warrant. Yet, according to Hayden, time would be of the essence and there would not be time to obtain a FISA warrant.[158] While FISA allows a seventy-two hour window to begin surveillance, a warrant application would still need to be prepared within seventy-two hours, and, more importantly, there must still be probable cause to begin the surveillance.[159] According to Hayden and Yoo, however, under conditions of hot pursuit, there may not be probable cause that the American is an agent of a terrorist group. He could just be an innocent contact of al-Qaeda or an agent of a terrorist group; surveillance is necessary to make that determination. As law professor Sims describes, "[t]he warrantless surveillance program is based on the fear that some relevant communications may slip through the cracks, in a situation in which the government either cannot get a FISA warrant or is unwilling to do so."[160]

---

[151] *NSA Hearings, supra* note 124, at 655.

[152] POSNER, *supra* note 144, at 94.

[153] YOO, *supra* note 78, at 106-107.

[154] *Id.* at 107.

[155] *Id.*

[156] *Id.* at 73.

[157] BAMFORD, *supra* note 134, at 110.

[158] *Id.*

[159] *Id.*

[160] SIMS, *supra* note 135, at 127-28.

Other hypothetical examples also highlight deficiencies with the probable cause standard. For instance, Senator Malcolm Wallop proposed the following scenario:

> Consider the case of someone with knowledge of a band of nuclear terrorists, hiding in one of a thousand apartments in a huge complex. It would be both reasonable and easy to tap every telephone in the complex, discard all intercepts but the correct one, and gain the vital information. But that would involve 999 violations of [FISA].[161]

Assistant Attorney General David Kris described a similar fact pattern during Congressional testimony:

> [I]f the government had probable cause that a terrorist possessed a nuclear bomb somewhere in Georgetown, and was awaiting telephone instructions on how to arm it for detonation, and if FISA were interpreted not to allow surveillance of every telephone in Georgetown in those circumstances, the President's assertion of Article II power to do so would be quite persuasive and attractive to most judges and probably most citizens.[162]

While these "ticking bomb" scenarios may be rare, and arguably farfetched, they do illustrate a potential problem with the probable cause standard that could justify rethinking the needed predicate for surveillance. Part V provides some thoughts about potential reforms.

B. *Procedural Requirements of FISA*

The second problem identified with FISA is the procedural requirements, which some commentators have described as overly burdensome. According to former DNI McConnell, FISA applications resemble "finished intelligence products" because they include "detailed facts describing the target of the surveillance, the target's activities, the terrorist network . . . and investigative results or intelligence information that would be relevant to the Court's findings," and are subjected to lawyers of review for legal and factual sufficiency.[163] According to former DNI General Counsel Benjamin Powell, the FISA process is cumbersome, necessitating substantial time and input from the "limited analysts and operators that are working these cases in real time."[164] Former Assistant Attorney General Wainstein estimated that the average FISA application is fifty

---

[161] *NSA Hearings, supra* note 124, at 865 n.96 (statement of David S. Kris, citing S. REP. No. 95-701, at 95-96 (1978)).

[162] *Id.* at 839.

[163] *Strengthening FISA Hearings, supra* note 66.

[164] *Modernization of the Foreign Intelligence Surveillance Act: Hearing on FISA Before the S. Comm. on Intelligence,* 110th Cong. 70-71 (2007) [hereinafter *Modernization of FISA Hearings*] (testimony of Benjamin A. Powell, Gen. Counsel, Office of the Dir. of Nat'l Intelligence).

to sixty pages long.[165]

FISA also has not kept up with technological advancements. For instance, as explained in Part I, the executive is allowed to conduct warrantless surveillance of foreign-to-foreign communications without a warrant.[166] When FISA was enacted in 1978, most such communications were conducted wirelessly.[167] Today, advances in technology have caused ninety percent of global communications to pass through fiber-optic cables and switching stations *on U.S. soil* which, according to the FISC in May 2007, requires a warrant.[168] McConnell posits that it takes approximately two-hundred man hours to obtain a FISA warrant for a foreign-to-foreign communication that happens to be routed through a cable in the United States.[169] If that same communication happened to occur wirelessly then no warrant would even be required. For example, in 2006, American soldiers were captured by Iraqi insurgents. Because most of the communications between the Iraqi insurgents were being routed through the United States, the government needed to obtain a FISA warrant to try to locate the soldiers even though all the parties to the surveillance were foreign nationals overseas.[170]

During the FISA Modernization Hearing in May 2007, McConnell noted that regulating communications based on the locus of collection arbitrarily limits the executive's ability to gather intelligence without offering any real Fourth Amendment protection.[171] Wainstein similarly argued that the government needed a "technology-neutral" framework for surveillance of foreign targets that focused not on "how a communication travels or where it is intercepted," but rather on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes."[172]

C. *Protect America Act*

In August 2007, based on the Bush administration's arguments that FISA was inadequate to fight the war on terror, Congress amended FISA with the Protect America Act (PAA) to allow warrantless surveillance of foreign-to-for-

---

[165] *Id.* at 70 (testimony of Hon. Kenneth L. Wainstein, Assistant Attorney Gen., U.S. Dep't of Justice).

[166] See *Katz* and *Keith* cases, discussed *supra* Section I.B. See also general discussion of FISA, *supra* at Section I.C.

[167] Joby Warrick & Walter Pincus, *How the Fight for Vast New Spying Powers Was Won*, WASH. POST, Aug. 12, 2007, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/08/11/AR2007081101349.html

[168] *Id.*

[169] BAMFORD, *supra* note 134, at 208.

[170] *Id.* at 300.

[171] *Modernization of FISA Hearings*, *supra* note 164 at 19 (testimony of Admiral J. Michael McConnell, Former Dir., Office of Dir. of Nat'l Intelligence).

[172] *Id.* at 46 (testimony of Hon. Kenneth L. Wainstein, Assistant Attorney Gen., U.S. Dep't of Justice).

eign communications that happened to be routed through the United States (considered non-controversial), as well as warrantless surveillance of U.S. citizens communicating with people overseas, as long as the target was reasonably believed to be located outside of the United States (considered controversial).[173] This Act corrected the technological problems concerning foreign-to-foreign communications being routed through the U.S. – such communications would no longer require a warrant. Yet, the Act also allowed warrantless surveillance of electronic communications between people *on* U.S. soil, including U.S. citizens, and people "'reasonably believed' to be overseas,"[174] without a court's order or oversight. Significantly, "the new law [gave] the attorney general and the director of national intelligence the power to approve the international surveillance," instead of the FISA court.[175] The FISC's only role was "to review and approve the procedures used by the government in the surveillance *after* it had been conducted."[176] Hence, the FISC did not scrutinize the cases of the individuals being monitored.

Despite the excoriation that the TSP received in the press and from prominent legal scholars, once Congress found out about the program, Congress did not cut funding to the NSA.[177] In fact, Congress even confirmed General Hayden (who had run the TSP for NSA) to head the CIA in 2006.[178] Moreover, Congress's passing of the PAA and the ultimate FAA, which essentially provides retroactive immunity to telecommunication providers and allows warrantless surveillance of Americans (as long as the intent is to acquire communications of non U.S. persons overseas),[179] has validated the underlying purpose of the TSP. In other words, although one can criticize the Bush administration for acting unilaterally and bypassing Congress and FISA, the underlying reasons for the TSP appear genuine and sound. If not, Congress could have taken more aggressive steps to reign in the program once it was revealed instead of passing legislation that retroactively condoned the warrantless surveillance.[180]

---

[173] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

[174] RISEN, *supra* note 130.

[175] *Id.*

[176] *Id.* (emphasis added).

[177] *See generally* Glenn Sulmasy & John Yoo, *Katz and the War on Terrorism*, 41 U.C. DAVIS L. REV. 1219, 1256-57 (Feb. 2008).

[178] On May 26, 2006, the Senate confirmed Hayden to be the Director of Central Intelligence. The vote was seventy-eight in favor, fifteen opposed, and seven did not vote. *See* U.S. Senate Roll Call Votes 109th Congress - 2nd Session, *available at* http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=109&session=2&vote=00160

[179] *See infra* Section IV.A for discussion of FAA provisions.

[180] While the Bush administration did inform Congress's "Gang of Eight" about the TSP in 2003, they were instructed not to consult with anyone else, including the intelligence committee's legal experts who had top-level clearances. It appears the Gang of Eight abided by this mandate. FISA presiding judge Royce Lamberth was also informed of the TSP but

The PAA was limited to six months because it was so controversial, and expired in February 2008.[181] In July 2008, Congress enacted the FAA. As explained in Part IV, the FAA borrowed several provisions from the PAA but added additional oversight mechanisms and more judicial review.[182] Nonetheless, the ACLU and several other civil liberty groups believe the FAA is unconstitutional and have filed suit in federal court.[183] As of this writing, the case is still pending. For the reasons explained below, this Article argues that the FAA is most likely lawful and appears to be a nuanced compromise between the legitimate need to expeditiously gather intelligence against terrorists, and the protection of Americans' civil liberties. In order to draw this conclusion, it is necessary to understand what traditional FISA requires, how the TSP program departed from that rubric, and how advances in technology and the nature of terrorism have impacted intelligence gathering.

PART IV: THE FISA AMENDMENTS ACT OF 2008

On July 9, 2008, Congress passed the FAA and President Bush signed it into law the next day.[184] It expires in 2012.

A. *Description of Key FAA Provisions*

Under the FAA, the Attorney General and the DNI may authorize jointly, for up to one year, the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[185] Importantly, the FAA expressly states that the surveillance "may not intentionally target any person known at the time of acquisition to be located in the United States[,]" "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States[,]" (a process known as "reverse targeting"), and "may not intentionally target a United States person reasonably believed to be located outside the United States."[186] Unlike the complicated provisions in FISA, which call for different treatment based on the kind of technology employed in acquiring the foreign

---

told he could not challenge it and had to keep it secret. While Lamberth believed he could not prevent the TSP or even disclose it, he did insist that the government flag any FISA requests that were based on the warrantless program. BAMFORD, *supra* note 134, at 116-17.

[181] Protect America Act of 2007, Pub. L. No. 110-55, § 6(c), 121 Stat. 552, 557.

[182] *See infra* Part IV.A discussing provisions of the FAA.

[183] Complaint at Amnesty v. McConnell, 08- cv-06259 (JKG) (S.D.N.Y. July 10, 2008). Complaint *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf

[184] FISA Amendments Act of 2008, Pub. L. No. 110-261, §403, 122 Stat. 2463, 2473 (2008).

[185] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § 1881a(a) (2008).

[186] *Id.* § 1881a(b)(1)-(3).

intelligence, the FAA declines to reference any particular technology. The Act instead specifies that acquisitions of communications must involve "the assistance of an electronic communication service provider."[187]

Although there are exceptions for exigent circumstances (as there are in FISA),[188] before the Attorney General and the DNI may authorize the targeting of foreign persons abroad under the FAA, they must first obtain a FISC order (e.g. a certification) approving the authorization.[189] Significantly, three requirements must be met for the FISC to issue such an order under the FAA. First, the FISC must find that the executive has "targeting procedures" in place that are reasonably designed to ensure that any acquisition conducted under the authorization is "limited to targeting persons reasonably believed to be located outside the United States," and will not intentionally acquire purely domestic communications.[190] Second, the FISC must find that the executive has minimization procedures in place for the acquisitions that meet FISA's requirements for such procedures.[191] Third, the Attorney General and the DNI must jointly certify, *inter alia*, that a "significant purpose" of the acquisitions is to obtain "foreign intelligence information."[192] "Foreign intelligence" is a term of art and encompasses sabotage, international terrorism, clandestine intelligence activities, and information relevant to national defense, security, or the conduct of foreign affairs.[193] If these requirements are met (and it appears the FISC can perform a de novo review of these certifications),[194] the FISC must authorize the surveillance within thirty days or request an extension for "good cause."[195] It appears that the FISC also performs an independent constitutional analysis to ensure the targeting is consistent with the Fourth Amendment,[196] although it is unclear what this additional requirement will add to the analysis, especially because foreign nationals overseas are not entitled to Fourth Amendment

---

[187] *Id.* § 1881a(g)(2)(A)(vi).

[188] *See* 50 U.S.C. § 1805(f) (2)(2000) (emergency wiretaps for seventy-two hours). The FAA increases the exigent circumstance exception from seventy-two hours to seven days. 50 U.S.C. §1881a(g)(1)(b). In other words, the government can initiate surveillance as long as the required certifications are presented to the FISC within seven days.

[189] 50 U.S.C. § 1881a(a), (i)(3).

[190] § 1881a(i)(2)(B).

[191] § 1881a(i)(2)(C); *see also* §§ 1801(h), 1821(4).

[192] § 1881a(g)(2)(A)(v).

[193] *See infra* note 45.

[194] The Protect America Act only required a "clearly erroneous" review so it appears the FAA gives more authority to the FISC, at least on paper. *See* §1881c(c)(3)(D) Given the ex parte nature of the proceedings, it is unclear whether a clearly erroneous review versus a de novo review will have much practical effect.

[195] Lydia Gensheimer, "HR6304 – Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008, *CQ Bill Analysis*, July 30, 2008.

[196] §1881a(b)(5) (all acquisitions "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States").

rights.[197]

At first blush, it seems that the FAA greatly expands the executive's ability to conduct surveillance in that there is no requirement, as there is under FISA, that the target be an agent of a foreign power.[198] Rather, the FAA essentially allows warrantless surveillance of foreign nationals reasonably believed to be overseas if a significant purpose of the acquisition is to gain foreign intelligence. Yet, it is incumbent to remember what FISA requires. FISA never called for FISC supervision or warrants for surveillance of foreign nationals overseas as long as the communications were wireless or the collection occurred on cables or wires overseas, and as long as the purpose was not to conduct surveillance on a known U.S. person in the United States. As explained previously, today many such foreign-to-foreign communications are now routed through the U.S., surveillance of which, according to the FISC, requires a warrant.[199] Under the FAA, as under the PAA, conversations between foreigners that are relayed through U.S. switching facilities are not subjected to FISA warrants.[200] Hence, the FAA appears to proceed in a technology-neutral and less arbitrary fashion; seen in this light, it does not seem that the FAA departs much from the underlying purpose of FISA.

In fact, in several ways, the FAA provides additional protection to U.S. persons as compared to FISA. Under the FAA, interceptions of international communications – which were never subjected to any FISC review if the communications were wireless or the wiretap occurred overseas – are now subjected to FISC oversight in the form of FISC-approved targeting and minimization procedures.[201] As Senator Orrin Hatch stated, "For the first time, the FISC will review and approve targeting procedures to ensure that authorized acquisitions are limited to persons outside of the United States. For the first time, the FISC will review and approve minimization techniques [for such acquisitions]."[202]

Furthermore, traditional FISA offers no statutory protection for U.S. persons abroad.[203] By contrast, the FAA prohibits the targeting of any U.S. person

---

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

[198] As explained earlier, the Fourth Amendment does not protect foreign nationals overseas. *See* Verdugo-Urquidez, 494 U.S at 271 (holding that only persons who "have come within the territory of the United States and developed substantial connections" to the country have Fourth Amendment rights).

[199] *See supra* note 167.

[200] *See generally* 50 U.S.C. § 1881a(b)(1)-(3) for a description of the communications requiring a FISA warrant under the FAA.

[201] 50 U.S.C. § 1881a(i)(2)(B) (targeting procedures);§ 1881a(i)(2)(C) (minimization procedures).

[202] 154 Cong. Rec. S6097, S6125 (Jun. 25, 2008).

[203] However, since 1981, surveillance against U.S. persons abroad has been regulated by executive order. Under Executive Order 12333, 46 Fed. Reg. 59941 (Dec. 4,1981), the executive may not conduct such surveillance using techniques that would require a warrant for law enforcement purposes, unless the "the Attorney General has determined in each case that

located outside the United States for foreign intelligence surveillance (where the person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes), unless the FISC has approved the surveillance based on a showing of probable cause to believe that the person is an agent of foreign power.[204] As Senator Diane Feinstein noted, "This bill does more than Congress has ever done before to protect Americans' privacy regardless of where they are, anywhere in the world."[205]

Despite these added protections for U.S. persons, the ACLU and several other civil liberty groups argue that U.S. persons' communications with individuals reasonably believed to be overseas will be intercepted without warrants and without probable cause. They argue that the collection of U.S. persons' communications is only exacerbated by the fact that the overseas targets do not even have to be agents of a foreign power.[206] At least under the TSP, there had to be a "reasonable basis" that at least one party to the communications was associated with al Qaeda.[207] Under the FAA, the government can conduct warrantless surveillance on any foreign national overseas, even with no connection to a terrorist group, as long as there is a significant purpose to gain foreign intelligence information.[208] Hence, civil liberties groups assert that the FAA is broader than the widely assumed illegal TSP because the government will be able to acquire all international communications of U.S. persons based on the theory that the surveillance is directed at obtaining foreign intelligence information, and targeted at people outside the United States.[209]

But if the executive engaged in such "reverse targeting" (where the purpose of the surveillance is really to monitor the conversations of U.S. persons), such an action would be illegal under the FAA.[210] Furthermore, it would also be an unwieldy means of gathering intelligence about a U.S. person, since only the person's communications with a foreign target abroad could be intercepted. As DNI McConnell argued to the Senate Judiciary Committee, "[F]or operational reasons, the Intelligence Community has little incentive to engage in reverse

---

there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power."

[204] 50 U.S.C. § 1881c(a)(2) (2008); *see also id.* §§ 1881b, 1881c.

[205] 154 Cong Rec. S6097, S6119 (Jun. 25, 2008).

[206] Memorandum in Support of Motion for Summary Judgment at 9, 27-29, Amnesty v. McConnell, 08- cv-06259 (JKG) (S.D.N.Y. Sept. 12, 2008).

[207] PRESS BRIEFING, *supra* note 94.

[208] *See* 50 U.S.C. § 1881a(a); § 1881a(g)(2)(A)(v). Under the TSP, Americans could be targeted without a warrant. Under the FAA, by contrast, Americans cannot be targeted without a receiving a traditional FISA warrant based on probable cause. 50 U.S.C. § 1881c(a)(2) (2008); *see also id.* §§ 1881b, 1881c.

[209] Memorandum in Support of Motion for Summary Judgment at 27-29, Amnesty v. McConnll, 08-cv-06259(S.D.N.Y. Sept. 12, 2008).

[210] *See* §1881a(b)(1).

targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique . . . ."[211]

In July 2008, the ACLU filed suit in the Southern District of New York arguing that the FAA violates the First and Fourth Amendments of the Constitution.[212] The plaintiffs in this lawsuit are attorneys and human-rights, labor, legal, and media organizations who allege that their work "requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, journalistic sources, witnesses, experts, foreign government officials, and victims of human rights abuses located outside the United States."[213] They posit that given "the scope of the challenged law," "the nature of their communications," and "the identities and geographic location" of the persons they communicate with, they "reasonably believe" that their communications will be "monitored" or "acquired, retained, analyzed, and disseminated" under the FAA.[214] Plaintiffs argue that this monitoring will cause a chilling effect and impede their ability to effectively communicate with people overseas.[215]

Yet, to the extent that FAA acquisition results in the incidental collection of information concerning U.S. persons communicating with the target of the surveillance, a non-U.S. person overseas, the FAA calls for FISC-approved minimization procedures (as does FISA) designed to prevent the unnecessary retention or dissemination of such information.[216] Significantly, the "incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment."[217] Similarly, in the context of a warrantless search, an officer may seize items within plain view as long as a warrant is not required to gain access to the search area in the first place.[218] It logically follows then that when the FAA targets non U.S. persons reasonably believed to be overseas who have no Fourth Amendment protection rights, there is no Fourth Amendment violation because the communications of U.S. persons are captured incidental to this lawful surveillance.

Nonetheless, the ACLU and others argue that the minimization procedures

---

[211] *Foreign Intelligence Surveillance Act and Implementation of the Protect America Act: Hearing before the S. Comm. on the Judiciary,* 110th Cong., (Sep. 25, 2007) (statement of J. Michael McConnell, Director of National Intelligence

[212] Complaint at Amnesty v. McConnell, 08- cv-06259 (JKG) (S.D.N.Y. July 10, 2008). Complaint *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf

[213] Memorandum in Support of Motion for Summary Judgment at 11, Amnesty v. McConnell, 08-cv-06259 (S.D.N.Y. Sept. 12, 2008); *see also* Complaint at ¶¶ 2, 44-45, Amnesty v. McConnell, 08-cv-06259 (S.D.N.Y Sept. 12, 2008).

[214] *Id.*

[215] *Id* at 12-14.

[216] 50 U.S.C. § 1881a(i)(2)(C); *see also* §§ 1801(h), 1821(4).

[217] United States v. Bin Laden, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000).

[218] Horton v. California, 496 U.S. 128, 135 (1990).

(which are the same minimization procedures under FISA) are ineffective and do not otherwise absolve the government of unlawful surveillance.[219] While minimization procedures are supposed to prevent the retention and dissemination of information that is not related to foreign intelligence, there are notable exceptions. Under the minimization procedures, "information that is evidence of a crime which has been, is being, or is about to be committed" can "be retained or disseminated for law enforcement purposes."[220] Furthermore, information such as a U.S. person's identity that is "necessary to understand foreign intelligence information" or needed to "assess its importance" can be retained.[221]

But the ACLU's position – that the government cannot conduct warrantless surveillance where one person happens, even incidentally, to be a U.S. person – puts the government in an untenable position. Essentially, it would require the executive to know in advance who a foreign national overseas plans to communicate with in the United States, so that the government can obtain a warrant when the foreign national calls. As Representative Randy Forbes stated during Congressional testimony:

> To require a court order for every instance in which a foreign target communicates with someone inside the United States is to require a court order for every foreign target, and requiring this would reverse 30 years of established intelligence gathering . . . . The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.[222]

Notwithstanding the problems laid out by Representative Forbes, there are legitimate concerns with the minimization procedures because a large number of incidental communications by innocent Americans will likely be acquired without any kind of warrant. As Georgetown law professor Marty Lederman notes, "the minimization requirements [under the FAA] are small solace: The government may not use or disseminate the information it *incidentally* obtains concerning U.S. persons . . . unless it has a (national security, foreign affairs or law enforcement) need to do so."[223] While Lederman acknowledges that the

---

[219] Reply in Support of Plaintiffs' Motion for Summary Judgment and Opposition to Defendants'' Cross-Motion for Summary Judgment at 1-2, Amnesty v. McConnell, 08- cv-06259 (JKG) (S.D.N.Y Dec. 12, 2008). *See* 50 U.S.C. § 1881a(i)(2)(C) (FAA minimization procedures); 50 U.S.C. §§ 1805(a)(3), 1801(h) (FISA minimization procedures).

[220] §1801(h)(3)

[221] §1801(h)(2).

[222] *Warrantless Surveillance and The Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II): Hearing before the H. Comm. on the Judiciary*, 110th Cong. 8 (2007)

[223] Posting of Marty Lederman to Balkinization, http://balkin.blogspot.com/2008/06/key-questions-about-new-fisa-bill.html (June 22, 2008, 20:27 EST) (emphasis in original).

minimization procedures are the same under FISA, he notes the potential consequences are more severe under the FAA because there is a "vastly expanded reservoir of foreign-to-domestic communications from which it can cull information about nontargeted U.S. persons."[224]

Yet, the FAA contains several forms of ex post oversight mechanisms that are absent from FISA and they might mitigate the risk that innocent Americans' communications will be acquired and retained. First, the FAA requires the Attorney General and the DNI to adopt guidelines used to train intelligence personnel concerning the implementation of the FAA's targeting restrictions. These measures are designed to ensure that the FAA is not used for surveillance of persons within the United States or at United States persons overseas.[225] Significantly, these guidelines must be provided to Congress and the FISC,[226] and must be adopted before any acquisitions may be authorized under the statute.[227] Furthermore, the FAA requires that the Attorney General and DNI assess the government's compliance with targeting and minimization procedures every six months and, submit the results to Congress and the FISC.[228] These assessments must include records of all proceedings before the FISC, any targeting and minimization procedures implemented during the assessment period, and any incidents of noncompliance with these procedures by any element of the intelligence community.[229]

Additionally, the FAA mandates that each agency of the intelligence community conducting surveillance report annually to the DNI, the Attorney General, Congress, and the FISC concerning its use of information obtained through the acquisitions.[230] Importantly, these reviews must establish the extent to which the acquisitions have collected the communications of U.S. persons, the number of disseminated intelligence reports resulting from these acquisitions that discuss an identified U.S. person, the number of additional U.S.-person identities subsequently disseminated in response to requests prompted by these reports, and the number of targets of these acquisitions who "were later determined to be located in the United States" at the time of the acquisitions and whose communications were reviewed.[231] Similarly, the FAA authorizes the Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community to acquire the information needed to conduct similar assessments.[232]

Finally, the FAA essentially provides immunity to the telecommunication

---

[224] *Id.*
[225] 50 U.S.C.§ 1881a(f)(1).
[226] *Id.* § 1881a(f)(2)
[227] *Id.* § 1881a(g)(2)(A)(iii).
[228] *Id.* § 1881a(l)(1).
[229] *Id.* § 1881f.
[230] *Id.* § 1881a(l)(3).
[231] *Id.* § 1881a(l)(3)(A).
[232] *Id.* § 1881a(l)(2).

providers who participated during the TSP. Participating telecommunication providers merely have to show a federal judge that they received written assurances from the Bush administration that the TSP was lawful.[233] Additionally, under the FAA, any electronic communication service provider ordered by the government to conduct surveillance is allowed to challenge the lawfulness of the directive in an adversarial proceeding before the FISC.[234] The provider can appeal any adverse decision to the FISCR and, on writ of certiorari, to the Supreme Court.[235]

B. *What is at Stake with the FAA?*

While civil liberties groups such as the ACLU argue that the FAA greatly expands executive power to conduct warrantless surveillance of Americans, a detailed analysis of the statute does not support the argument that the FAA, as written, is that much of a departure from traditional FISA. The better argument for the ACLU and other critics is that traditional FISA did not adequately address the issue of international communications between U.S. persons in America and foreign nationals overseas – not that the FAA is a significant departure from the underlying rationale of FISA. Importantly, under traditional FISA, the government could conduct warrantless surveillance of foreign nationals overseas, even if they happened to speak to a U.S. person in the United States, as long as the technology was wireless or the wiretap occurred abroad.

Undoubtedly, there is potential for abuse if executive officials bypass the clear statutory provisions of the FAA. Yet, it does not appear that the FAA, as written, is unconstitutional, and in many significant ways it enhances protections for U.S. persons. Of course, just because a statute, as written, appears constitutional and lawful does not mean it will be implemented as such. For instance, in March 2007, a Justice Department inspector general report found that the FBI had improperly used the Patriot Act to gather telephone, bank and other information about U.S. citizens.[236] Furthermore, in October 2008, some NSA agents claimed that, under the TSP, they were ordered to intercept and transcribe international communications between American service members in the Middle East and their spouses/significant others in the United States.[237] This information, if true, contradicts the statements by the Bush administration that the TSP program only targeted suspected terrorists.[238] After these revelations came to light, Senators Patrick Leahy and Arlen Specter requested that

---

[233] *Id.* §1885a(a)(4).

[234] *Id.* §1881a(h)(4)(A).

[235] *Id.* § 1881a(h)(4)(6).

[236] David Stout, *FBI Head Admits Mistakes in Use of Security Act*, N.Y. TIMES, March 10, 2007, at A1.

[237] *Leahy, Spencer Push DNI and NSA to Investigate Wiretapping Allegations*, CONGRESSIONAL DOCUMENTS, Oct. 10, 2008, *available at* 2008 WLNR 19492834.

[238] *See, e.g.*, PRESS BRIEFING, *supra* note 94.

former DNI McConnell conduct a full investigation of the allegations, provide written assurances that "ill-gotten information" concerning Americans was properly destroyed or removed from government databases, and provide a list of steps taken to ensure that the same mistakes do not reoccur.[239] Yet, unlike the secret TSP, the FAA has detailed ex post review and oversight mechanisms embedded in the legislation that would presumably detect and deter such abuse. It is also important to remember that the "Fourth Amendment demands reasonableness, not perfection."[240]

In sum, under traditional FISA, certain kinds of international communications have always been completely outside of FISA review. Under the FAA, there is now FISC reviews of targeting and minimization procedures as well as the ex post oversight mechanisms. Additionally, it is not even clear that a warrant would be required to gather foreign intelligence within the country. While per *Keith,* a warrant is required if the threat is solely domestic, it is unsettled whether a warrant is required when there is a connection to a foreign power. Significantly, in August 2008, the FISCR upheld the constitutionality of the PAA (that had expired) explicitly finding that there was a foreign intelligence exception to the Fourth Amendment warrant requirement.[241] Although the petitioners (telecommunication companies who did not want to comply with an order under the PAA) argued that the PAA would result in incidental communications of innocent Americans being retained due to warrantless surveillance of people reasonably believed to be overseas, the FISCR rejected that argument. It stated, "The petitioner's concern of incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[242]

The FISCR's holding that the PAA was constitutional means that it would likely find the FAA – which has more judicial review and reporting requirements than the PAA – to be similarly lawful. Hence, it seems a legal stretch to maintain that the government needs a warrant when it targets foreign nationals overseas who may incidentally communicate with U.S. persons in the United States. While the FAA, as applied to U.S. persons, must still be reasonable under the Fourth Amendment, given the FISC-monitored minimization procedures and ex post oversight mechanisms, it seems that the FAA has struck a

---

[239] *Leahy, Spencer Push DNI and NSA to Investigate Wiretapping Allegations, supra* note 237.

[240] Pasiewicz v. Lake Cty. Forest Preserve Dist., 270 F.3d 520, 525 (7th Cir. 2001).

[241] *In re Directives * Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, No. 08-01, 15, 17 (FISA Ct. Rev. Aug. 22, 2008) (while applying principles derived from the special needs cases, the FISCR concluded "that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States").

[242] *Id* at 26 (citations omitted).

nuanced compromise between the need to expeditiously gather foreign intelligence, and the protection of civil liberties.

Furthermore, compared to traditional FISA, the FAA relies more heavily on ex post oversight mechanisms than on ex ante warrants based on individualized suspicion—and this may be a benefit. Several scholars have questioned the effectiveness of FISA's ex ante warrants issued by a secret court based on only one-sided information provided by the government.[243] Critics of FISA argue that because the FISC approves virtually all requests for warrants, it merely serves as a rubber stamp and does not provide any genuine judicial review. The FISC has, indeed, approved almost all warrant requests—as of 2006, the FISC had approved all but five out of over 17,000 requests.[244] According to a Note written by the *Harvard Law Review*, ex ante judicial review to conduct foreign surveillance may be counterproductive and unworkable:

> The [FISC] judge lacks a skeptical advocate to vet the government's legal arguments, which is of crucial significance when the government is always able to claim the weight of national security expertise for its position. It is questionable whether courts can play this role effectively, and, more importantly, whether they should.[245]

Because the FISC has no way to evaluate the facts presented by the government, it has to assume that the government-provided facts are correct. Problematically, the FISC identified evidence of governmental misstatements and omissions of material facts in seventy-five FISA applications.[246] This evidence did not come to light until after the FISC issued the warrants.[247]

Judges are also extremely deferential to claims of national security, especially when they "must weigh the national security necessity ex ante, rather than being asked to review it after the fact."[248] The Harvard Note argues that "[e]x ante judicial review is not only of limited effectiveness, but it is also affirmatively harmful" in that it "imparts a broader imprimatur of validity than is warranted given the limited effectiveness of judicial review."[249] Hence, as the Note observes, ex ante judicial review may impede security without providing any real privacy interest protection.[250] Therefore, the Note argues that "Congress is better situated constitutionally and better equipped institutionally to make the sort of value judgments and political determinations that are necessa-

---

[243] Note, *Shifting the FISA Paradigm: Protecting Civil Liberties by Eliminating Ex Ante Judicial Approval*, 121 HARV. L. REV. 2200, 2207 (2008).

[244] Johnson, "NSA Spying Erodes Rule of Law," 411.

[245] Note, *supra* note 243.

[246] *Id.* at 2207-08.

[247] *Id.* at 2208.

[248] *Id.* at 2209.

[249] *Id.* at 2211.

[250] *Id.* at 2011-12.

ry to fulfill FISA's purposes."[251] The Note concludes that "[t]hose concerned with protecting civil liberties should view an end to reliance on ex ante judicial review as a chance to develop real political checks that can vigorously protect both national security and liberty interests."[252]

If the Note's assertions are true, the FAA has one advantage over the traditional FISA in that the FAA relies more on ex post mechanisms. For example, the FAA imposes reporting requirements to Congress[253] and inspector general reviews,[254] rather than relying solely on ex ante warrants issued by a secret court. While under the FAA the FISC issues ex ante certifications concerning the executive's targeting and minimization procedures, these are programmatic reviews and not based on individualized suspicion of suspects as is required by traditional FISA. Given the arguably limited effectiveness of ex ante warrants issued by a secret court based on one-sided evidence, the FAA's greater reliance on ex post review mechanisms could be viewed as a significant improvement over traditional FISA. As Georgetown law professor Neal Katyal observed, "[r]eporting requirements are powerful devices" that promote external checks on excessive executive power.[255]

In contrast, the high degree of judicial deference in ex ante review may simply result from quality applications. Applications for traditional FISA warrants must survive considerable review by the executive branch prior to submission to the FISC; hence, it can be presumed that some, if not many, applications are not brought. As Alan Dershowitz notes, "[a]lthough the FISA court has only rarely denied requests for national security wiretaps, the very existence of this court and the requirement of sworn justification serves as a check on the improper use of the powerful and intrusive technologies that are permitted in national security cases."[256] Hence, there are two ways to look at ex ante review: one could either argue that FISA "force[s] the [e]xecutive to self-censor its requests," or that the judiciary is "act[ing] merely as a 'rubber stamp.'"[257] The reality is probably a little of both.

The FAA contains both ex ante and newly imposed ex post review mechanisms. While the ex ante review under the FAA is not based on individualized determinations about suspects, but rather focuses on programmatic reviews, because of its heavy ex post reporting mechanisms, it seems that the FAA creates

---

[251] *Id.* at 2217.

[252] *Id.* at 2221 (emphasis added).

[253] *See* 50 U.S.C. § 1881f (outlining congressional oversight).

[254] *See id.* § 1881a(l) (identifying assessments and reviews).

[255] Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L J 2314, 2342 (2006).

[256] Alan Dershowitz, "A Stick with Two Ends," *Opening Argument* (Yale Law School), Feb. 2006, at 404, *available at* http://openingargument.com/index.php?name=Home&file=article&did=68.

[257] Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1397 (1993).

a balanced structure that may prevent executive branch abuse while still protecting the nation from another terrorist attack.

President Obama voted in favor of the FAA while still in the U.S. Senate, but stated that he would ask his attorney general to review the bill if elected President:

> Given the choice between voting for an improved yet imperfect bill, and losing important surveillance tools, I've chosen to support the current compromise . . . I do so with the firm intention – once I'm sworn is as president – to have my attorney general conduct a comprehensive review of all our surveillance programs, and to make further recommendations on any steps needed to preserve civil liberties and to prevent executive branch abuse in the future.[258]

This Article suggests that while there is potential for abuse if government officials violate the clear wording of the FAA (which allows warrantless surveillance of non-US persons reasonably believed to be outside the United States to gather foreign intelligence), the FAA contains enough ex post review mechanisms (in the forms of Congressional oversight committees and various inspectors general) that the Obama administration should allow the FAA to operate as-is, and reevaluate its effectiveness and protection of civil liberties when it expires in 2012.

PART V: AREAS FOR FUTURE REFORM

When the Obama administration does revisit the FAA, there are two areas of weakness it should address: (1) handling mere contacts with suspected al Qaeda agents (addressed in Part III) and (2) dealing with the potentially vast number of incidental communications by U.S. persons acquired without a warrant (addressed in Part IV).

A. *Contacts with Al Qaeda Agents*

The FAA solves the technological problem associated with foreign-to-foreign communications being routed through America. Unfortunately, it does not appear to adequately address the concern that U.S. persons unaffiliated with foreign powers may be subjected to warrantless surveillance after being contacted by foreign terrorist suspects. For instance, if the purpose of the FAA was in part to solve the problems discussed in Part III concerning an overseas terrorist calling ten phone numbers in America,[259] it does not seem that the FAA resolves that issue. Under the FAA, while there is no need for a warrant to target the alleged overseas terrorist (who does not even need to be a terrorist but just a foreign national);[260] it does require the executive branch to obtain a

---

[258] BAMFORD, *supra* note 134, at 308.

[259] YOO, *supra* note 78, at 105.

[260] *See* 50 U.S.C. § 1881a(a).

FISA warrant before conducting follow-up surveillance on the U.S. person who answered the phone.[261] Under the FAA, as soon as the government *targets* a U.S. person (no matter where located), the executive must show probable cause that the U.S. person is an agent of a foreign power.[262]

One solution to this problem is to use the equivalent of a "*Terry* stop" for electronic surveillance–a solution proposed by Kim Taipale, Executive Director of the Center for Advanced Studies in Science and Technology Policy. As Taipale explains, "where collateral U.S. person communications are intercepted incidental to a legitimate foreign intelligence intercept, there is no explicit way consistent with FISA . . . to engage in follow up electronic surveillance to determine if probable cause exists to target the individual, even though the collateral intercept itself may give rise to a constitutionally reasonable suspicion."[263] Pursuant to the seminal case *Terry v. Ohio*,[264] a police officer can briefly detain a person for questioning and conduct a limited pat-down frisk if the officer has "reasonable suspicion" (a standard less than probable cause) to believe that the person may be involved in a crime.[265] If the *Terry* stop reveals additional evidence of a crime, that evidence can be used to justify probable cause and a full-scale search or arrest.[266] In the case of electronic surveillance, a "*Terry* stop" would allow an authorized period for additional monitoring or initial investigation of the U.S. person in contact with the alleged terrorist.[267] In other words, in the case of a terrorist who calls a U.S. person, the government could briefly perform follow-up surveillance on the U.S. person to determine whether the communications have any intelligence value. If this follow-up surveillance revealed that the U.S. person was an agent of a foreign power, then a traditional FISA warrant could be obtained based on probable cause. If the U.S. person's communication was innocent, then the follow-up surveillance would be minimized.

CATO Senior Fellow Robert Levy made a similar suggestion to the Senate Judiciary Committee in February 2006. He suggested that "FISA could be amended so that warrants could issue merely upon showing that an individual

---

261 *See* 50 U.S.C. § 1881a(b) (describing limitations to the Attorney General and Director of National Intelligence's authority under the FAA)

262 50 U.S.C. § 1881b(c)(1)(B)(ii).

263 K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J.T. & TECH. 128 (Spring 2007) (citations omitted).

264 392 U.S. 1 (1968).

265 *Id.* at 30.

266 *Id.*

267 Foreign Intelligence Surveillance Act Reform, Open Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) Before the H. Permanent Select Comm. on Intelligence (HPSCI), at 6 (Jul. 19, 2006) (testimony of Kim Taipale, Executive Director of the Center for Advanced Studies in Science and Technology), *available at* http://intelligence.house.gov/Reports.aspx?Section=141.

has had contact with al Qaeda."[268] Both Taipale's and Levy's solutions would rely on individualized ex ante review by the FISC; however, each expert would change the inquiry or standard that the judiciary employs.

Judge Posner suggests a more radical approach. He would allow warrantless international and domestic surveillance of Americans without basis on any ex ante predicate standard or an attenuated standard, like a "reason to believe that the surveillance might yield clues to terrorist identities, plans, or connections."[269] Yet, Judge Posner notes that the more watered-down the predicate standard, the less meaningful role it plays in deterring abuse: "If all that the government is required to state in its application is that it thinks an interception might yield intelligence information, judges will have no basis for refusing to grant the application."[270] Instead, Judge Posner would rely more on ex post review and reporting mechanisms to control abuse.[271] He would also prevent law enforcement personnel from using information gleaned by warrantless surveillance for most non-national security related crimes.[272] For example, if an intelligence officer overheard a man discussing a murder (not related to terrorism), the officer would have to minimize and ignore such communication as it would not be related to national security. As Posner explains, "[i]t is more important that the public tolerate extensive national security surveillance of communications, than that an occasional run-of-the-mill crime go unpunished because intelligence officers were not permitted to share evidence of such a crime with law enforcement authorities."[273] In other words, Posner's solution would rely on minimal, if any, ex ante review mechanisms and instead rely on extensive ex post reviews to deter and prevent governmental abuse of warrantless surveillance information.

Under the Fourth Amendment, warrants require probable cause.[274] Some argue that the warrant requirement is unworkable in the national security context. For example, if the initial determination of an individual's status as a foreign power agent requires surveillance, then probable cause for such surveillance will rarely exist. And, although the Fourth Amendment does not require warrants in all cases, surveillance must at least be reasonable under the circumstances.[275] As attorney David Rivken notes:

---

[268] LEVY, *supra* note 124, at 8.

[269] POSNER, *supra* note 144, at 101.

[270] POSNER, *supra* note 147, at A16.

[271] For details of Judge Posner's ex post review, which includes a steering committee and biannual reviews to the FISC, please *see id.*

[272] *See id.*

[273] POSNER, *supra* note 144, at 99. Posner, however, does suggest that exceptions unrelated to terrorism may be appropriate for serious crimes such as serial murder. *Id.*

[274] *See* U.S. CONST. amend. IV (stating that "no Warrants shall issue, but upon probable cause").

[275] *See generally* Illinois v. Rodriguez, 497 U.S. 177 (1990) (consent exception); Coolidge v. New Hampshire, 403 U.S. 443 (1971) (plain view exception); Illinois v. McArthur,

> While the Executive can constitutionally carry out a "reasonable" search that infringes on personal privacy, a warrant cannot be granted by a court absent "probable cause." Applying the higher probable cause standard would mean that NSA could only surveil the conversations of full-fledged al Qaeda agents, leaving invaluable conversations among al Qaeda sympathizers unmonitored.[276]

Therefore, similar to Posner's approach, Rivken recommends political accountability to deal with abuses but not necessarily ex ante reviews based on probable cause. He suggests that Congress cut off the funds for NSA surveillance as one way to control NSA abuses.[277]

Although Posner and Rivken make persuasive arguments, it is not clear that we should eliminate all ex ante review, because it encourages the executive to self-censor its surveillance requests; therefore, the ex ante review process may contain inherent benefits. Yet, the ex ante inquiry need not require probable cause that the target is an agent of a foreign power. We could modify the probable cause inquiry and still retain the benefits associated with FISC ex ante review of surveillance requests.

The traditional "*Terry* stop" provides a useful analogy for potential FISA and FAA modification. When trying to decide whether a warrantless search is justified, law enforcement personnel ask whether probable cause exists to suspect that the individual has committed or is about to commit a crime. When trying to decide whether warrantless surveillance is justified, for foreign intelligence purposes, the question is whether there is probable cause to suspect that the individual is an agent of a foreign power. Perhaps, Congress should amend FISA to require probable cause that a terrorist (not just a foreign national as the FAA currently requires) has had contact with a U.S. person. If that standard is met, then Taipale's solution of a "*Terry* stop" could be used to continue surveillance for an initial period on the U.S. person to determine if he is a terrorist. In other words, probable cause could still be the predicate standard for FISC ex ante review– but it would apply to a very different inquiry than is currently required under FISA and the FAA.

This *Terry* stop surveillance approach is likely constitutional. The Supreme Court held in *Keith* that the standard of probable cause needed to obtain warrants for intelligence purposes could be different from the traditional standard used for law enforcement: "Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need

---

531 U.S. 326 (2001) (exigent circumstance exception); Chimel v. California, 395 U.S. 752 (1969) (incident to lawful arrest exception); Carroll v. United States, 267 U.S. 132 (1925) (automobile exception); New Jersey v. T. L. O., 469 U.S. 325 (1985) (public schools exception); United States v. Flores-Montano, 541 U.S. 149 (2004) (border-search exception).

[276] David B. Rivkin, Jr., *Much Ado About Nothing*, *in* INTELLIGENCE AND NATIONAL SECURITY, THE SECRET WORLD OF SPIES, *supra* note 32, at 408.

[277] *Id.*

of Government for intelligence information and the protected rights of our citizens."[278] Hence, there is an argument that one could reframe the question of probable cause from whether the target is an agent of a foreign power to whether the target has been contacted by a terrorist. In other words, the probable cause that FISA requires is probably higher than what is required under the Fourth Amendment.

Similarly, in terms of the other hypothetical situations discussed in Section III,[279] the question could be rephrased as "whether probable cause that wiretapping all 1000 apartments would stop the attack, or whether wiretapping the phones in Georgetown would avert a nuclear disaster." Such an approach would, indeed, be lawful. According to Posner, the Supreme Court has suggested that a dragnet search of every car in an area to locate a bomb would not violate the Fourth Amendment, even though there would not be probable cause or even reasonable suspicion to suspect any individual car.[280] Posner believes that the Court would reason that the delay, inconvenience, and privacy intrusion to the drivers would be outweighed by the danger of a bomb.[281] The situation involving surveillance to stop a nuclear bomb is even more compelling.

In sum, when evaluating the FAA and considering additional surveillance reform, Congress should consider creating a policy that allows officials to investigate mere contacts with terrorists without first requiring probable cause to believe that the contact is an agent of a foreign power. One possible reform could change when intelligence officials are required to use the probable cause standard. Another way, as suggested by Judge Posner, would be to relax the ex ante inquiry and allow widespread warrantless surveillance but rely more heavily on ex post mechanisms to deter and detect abuse.[282]

B. *Incidental Communications of U.S. Persons*

Under the FAA, the potential exists that vast numbers of incidental communications made by U.S. persons will be acquired, especially because the executive can conduct warrantless surveillance of foreign nationals overseas who may happen to communicate with a U.S. person. While the FAA requires minimization procedures, as explained in Part IV, there are plenty of exceptions.[283] One way to obviate the concerns of civil libertarians, who worry that information obtained through warrantless surveillance used to gather foreign intelligence could be used to prosecute domestic crimes, is to add statutory language limiting the crimes that could be prosecuted using evidence gathered under the FAA. In other words, officials could use information concerning terrorism for

---

[278] *Keith*, 407 U.S. at 322-23.

[279] *See supra* notes 161-62 describing hypothetical problems under FISA.

[280] POSNER, *supra* note 144, at 90.

[281] *Id.*

[282] POSNER, *supra* note 144, at 101.

[283] 50 U.S.C. §1801(h)(2) & (3).

prosecution, but information concerning crimes unrelated to terrorism would not be given to law enforcement officials. Law professor Banks proposes a solution calling it an "exclusionary rule for FISA."[284] Under this proposal, the "government would be prevented from using FISA-obtained information as evidence in a prosecution of a target for a so-called collateral crime–one having nothing to do with terrorism or national security."[285] Such an exclusionary rule might mitigate potential abuse of the acquisitions of incidental U.S. communications pursuant to the FAA and would not undermine national security.

A second potential problem with collecting vast amounts of data concerns efficacy. Jerry Berman and Lara Flint from the Center of Democracy and Technology argue that September 11 was not a result of lacking the right intelligence but rather a result of the government not making effective use of the information already in its possession, and failing to adequately share information among government agencies.[286] Berman and Flint argue, "[g]ranting the government broader authority to collect vastly greater volumes of information without particularized suspicion could exacerbate this problem."[287] Journalist James Bamford reaches a similar conclusion: "Those involved in the warrantless eavesdropping operation soon began to realize its limitations. By gaining speed and freedom, they sacrificed order and understanding."[288] Part of the challenge is recognizing when incidental communications become foreign intelligence. As the court noted in *United States v. Rahman*:

> [W]hen the purpose of surveillance is to gather intelligence about international terrorism, greater flexibility in acquiring and storing information is necessary, because innocent-sounding conversations may later prove to be highly significant, and because individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time.[289]

Therefore, one outstanding question that will need to be addressed when the FAA is revisited is whether, through the FAA, the government is capturing actionable intelligence or acquiring so much data that the FAA's effectiveness is undermined.

CONCLUSION

Law professor Banks argues that FISA was a compromise allowing secret electronic surveillance to collect foreign intelligence, while subjecting such ap-

---

[284] BANKS, *supra* note 41, at 1291.

[285] *Id.*

[286] Jerry Berman & Lara Flint, *Guiding Lights: Intelligence Oversight and Control for the Challenge of Terrorism*, 22 Crim. Just. Ethics 2, 2 (2003).

[287] *Id.*

[288] BAMFORD, *supra* note 134, at 122.

[289] *United States v. Rahman*, 861 F.Supp. 247, 252-53 (S.D.N.Y. 1994).

plications to judicial warrants and Congressional oversight.[290] According to Banks, this central premise of FISA has been lost by the "cumulative complexity" of the statute, challenges of new technology, the Bush administration's TSP program, and the efforts to amend and curtail FISA's provisions.[291] Yet, FISA's situation does not appear to be as dire as Banks might suggest. FISA was generally not intended to cover international communications, even those involving U.S. persons, if the intent was to target a foreign national overseas. It seems simply irrelevant to privacy and liberty concerns whether the communications occur via fiber optic cable or wireless communication, or whether the acquisition takes place domestically or overseas. While the FAA has corrected some of these technological anomalies with FISA, other areas are in need of reform, such as surveillance of mere contacts with terrorists. While it is certainly understandable that the ACLU and others fear that the FAA could result in the acquisition of vast amounts of innocent communications made by U.S. persons, this Article suggests that the real issue posed by the FAA is not so much the substantive provisions of the FAA but rather the lack of trust in the executives who will be implementing its provisions. If true, then, ironically, the best strategy for improving secret surveillance may be to create a more transparent government.

---

[290] *See* BANKS, *supra* note 41.

[291] *Id.* at 1214-1215.