I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Surveillance and Privacy Under the Obama Administration: The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 and the Attorney General's Guidelines for Domestic FBI Operations

ELIZABETH JOHNSON*

Abstract: President Obama faces the challenge of balancing intelligence gathering and surveillance with civil rights and privacy. This note discusses the intersection between surveillance and privacy vis-à-vis the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 and the Attorney General's Guidelines for Domestic FBI Operations, two recently adopted documents that serve as a framework for the President's efforts.

The Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 was enacted to address surveillance conducted in accordance with the Patriot Act and the Protect America Act, with the specific aim of establishing a procedure for authorizing certain acquisitions of foreign intelligence. It also addresses both the President's ability to conduct surveillance as he deems necessary and the telecommunications industry actors who have previously conducted surveillance by direction of the President.

The Attorney General's Guidelines for Domestic FBI Operations are focused on FBI intelligence gathering operations within the United States for threats to national security. The 2008 Guidelines were enacted with the specific goals of expanding FBI intelligence gathering capabilities, protecting the United States against terrorism, and bringing FBI domestic procedures to light in order to reassure the

*Elizabeth Johnson is a 2010 J.D. candidate at The Ohio State University Michael E. Moritz College of Law.

American people that the FBI acts in accordance with the law.

Both documents were carefully crafted to protect the United States by maximizing intelligence gathering and surveillance capabilities while continuing to protect civil rights and individual privacy. This Note discusses how the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 and the 2008 Guidelines depart from previous versions and addresses key issues going forward.

INTRODUCTION

President Obama wants to "improve intelligence capacity and protect civil liberties."[1] Two legal frameworks structure the President's effort to improve surveillance and intelligence gathering to combat terrorism, while at the same time protecting privacy and civil rights:[2] (1) the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ("FISA Amendments Act of 2008") and (2) the Attorney General's Guidelines for Domestic FBI Operations (the "2008 Guidelines").

FISA and the Guidelines emerged out of the Watergate scandal and Church Committee era and represented an attempt to prevent excessive surveillance by the executive.[3] Following the Watergate scandal, the Senate Select Committee, chaired by Frank Church, initiated a study to investigate government operations and domestic intelligence activities.[4] The Church Committee found that the intelligence agencies sometimes warped intelligence to meet political goals and in 1976 recommended "to limit the FBI to investigating

---

[1] White House Agenda, http://www.whitehouse.gov/agenda/homeland_security (last visited April 13, 2010).

[2] According to Attorney General Holder, "We must strengthen the activities of the federal government as we protect the people—the American people—from terrorism. Nothing we do will be more important. We must use every available tactic to defeat our adversaries – and we must do so within the letter and the spirit of the Constitution. There is not a tension between the ideals that formed this nation and that which we must do to keep it safe." Department of Justice, http://www.usdoj.gov/ag/speeches/2009/ag-speech-090203.html (last visited April 13, 2010).

[3] *See* Peter Swire, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy, & The USA Patriot Act: Surveillance Law: Reshaping the Framework: The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (1994) for a more complete discussion on the history of surveillance in America.

[4] *Id.* at 1316.

conduct rather than ideas or associations."[5] In response to the findings of the Church Committee, Attorney General Edward Levi issued his Guidelines on Domestic Surveillance in 1976 ("Levi Guidelines"), setting limits on domestic surveillance investigations.[6] The Levi Guidelines gave the Justice Department oversight of the FBI and explicitly stated that FBI investigations were "not to limit the full exercise of rights protected by the Constitution and laws of the United States."[7] Congress passed FISA in 1978, in the wake of Watergate and the Church Committee findings, to describe the requirements for conducting foreign electronic surveillance.[8] The legislation was a compromise between maximum flexibility in protecting national security and maximum regulation to ensure the protection of civil rights.[9]

The attacks of September 11, 2001 created the most pressure since the 1970s in favor of greater government surveillance, leading to major modifications to both the Guidelines and FISA. The Obama Administration must now decide whether the policies of the 1970s or the September 11 era should be the proper model for ensuring the improvement of the nation's intelligence gathering capability while protecting the civil liberties of the American people.

I. FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACT OF 2008

A. HISTORY OF FISA

Congress enacted FISA in 1978 to regulate electronic surveillance activities within the United States for foreign intelligence purposes.[10] Congress passed FISA as a means of balancing the need for government surveillance with Fourth Amendment protections.[11] Prior

---

[5] *Id.* at 1319-1320.

[6] *Id.* at 1326.

[7] *Id.*

[8] *Id.* at 1315.

[9] *Id.* at 1320.

[10] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-71 (2006).

[11] Swire, *supra* note 3, at 1320.

to FISA, it was not uncommon for the President to exercise a "national security exception" to the Fourth Amendment's warrant requirement, conducting electronic surveillance as he deemed necessary.[12] Congress passed FISA after the Watergate scandal exposed the abuses of such warrantless electronic surveillance.[13]

Consistent with its original purpose, FISA continues to provide procedural guidelines for obtaining a court order (called a "FISA order") for a particular surveillance activity.[14] FISA also establishes the framework within which foreign electronic surveillance is to be conducted.[15] As the codification of foreign electronic surveillance procedures, FISA protects civil rights by providing judicial and congressional oversight of surveillance actions.[16]

In the 1978 FISA, Congress created judicial oversight with the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review ("FISCR").[17] The intelligence agency seeking to perform foreign intelligence surveillance within the United States would apply before an individual FISC judge in order to receive the FISA order.[18] If the order was denied, the intelligence agency was not permitted to apply to another of the seven appointed judges; instead, the agency could appeal to the FISCR, a three-judge panel whose sole jurisdiction lies in reviewing denied applications for FISA orders.[19] Periodic reports to congressional committees provided congressional oversight over the FISA review process.[20]

---

[12] 190 A.L.R. Fed. 385, § 2[a].

[13] *Id.* When FISA was passed in 1978, then-Attorney General Griffin Bell emphasized that it "does not take away the power of the president under the Constitution."

[14] 50 U.S.C. § 1805 (2006).

[15] *Id.*

[16] *Id.* at §§ 1807-1808.

[17] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978), § 103(a).

[18] *Id.* at § 104.

[19] *Id.* at § 103. The seven district court judges were to be publicly appointed by the Chief Justice of the United States Supreme Court from seven of the U.S. judicial circuits. The three judges on the FISCR were to be appointed by the Chief Justice from the U.S. District Courts or Courts of Appeals.

[20] *Id.* at § 108.

After the September 11, 2001 terrorist attacks, Congress amended FISA with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act").[21] The terrorist attacks revealed that even the United States "might be penetrated and devastated by a small band of determined zealots," and Congress acted quickly to enhance government powers of investigation.[22] One of the Patriot Act's primary impacts on FISA was expanding the purposes for which surveillance could be conducted.[23] In 1978, FISA authorized a FISA order only if the "primary purpose" of the order was to obtain foreign intelligence information.[24] This created a "wall" between law enforcement and foreign intelligence investigations.[25] The Patriot Act permits a FISA order if a "significant purpose" of the surveillance is to obtain foreign intelligence information.[26] Under the "significant purpose" paradigm, as long as a foreign intelligence information nexus exists, a FISA order would be granted under the Patriot Act even though the evidence gathered may also be intended for use in a criminal prosecution.[27] The line between domestic criminal investigations and foreign surveillance operations thus began to blur.[28]

A FISA order is analogous to a domestic search warrant under the Fourth Amendment, but the "significant purpose" requirement under the Patriot Act arguably limits Fourth Amendment protections.[29] For example, the FBI can gather evidence through a FISA-ordered

---

[21] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[22] Lisa Finnegan Abdolian and Harold Takooshian, *The USA Patriot Act: Civil Liberties, the Media, and Public Opinion*, 30 FORDHAM URB. L.J. 1429, 1429 (2003).

[23] Swire, *supra* note 3, at 1330. The Patriot Act also expanded the FISC from seven to eleven judges. USA PATRIOT Act, Pub. L. No. 107-56, § 208.

[24] Swire, *supra* note 3, at 1330.

[25] *Id.*

[26] *Id.*

[27] Clifford S. Fishman and Anne T. McKenna, Wiretapping & Eavesdropping Database, WIRETAP § 1:17, April 2009, *available at* www.westlaw.com.

[28] *Id.*

[29] Jennifer C. Evans, Note, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L. J. 933, 974 (2002).

surveillance activity by showing that the foreign intelligence is a significant purpose of the search. Specifically, the FBI can use the evidence to prosecute a crime without ever having to show probable cause.[30] Conversely, some argue that the Patriot Act expands government surveillance at the expense of individual liberties through this treatment of probable cause.[31]

Even with the expanded government surveillance power under the Patriot Act, the President may continue to exercise his "national security exception" and conduct foreign surveillance as necessary.[32] This power was the subject of public debate that centered on whether Article II of the Constitution allowed the President to carry out this exception to FISA.[33] Every court of appeals that has addressed the issue found that the President does have an inherent power to authorize warrantless foreign intelligence surveillance.[34] In 2002, the FISCR agreed that "the president does have that authority" and noted that "FISA could not encroach on the president's constitutional power."[35]

The Protect America Act ("PAA") was enacted in 2007 in the midst of the presidential "national security exception" debate.[36] It granted authority to the United States Attorney General and Director of National Intelligence to conduct surveillance of persons located outside the United States for one year without a FISA order.[37] Instead of asking the FISA court for an order, the Attorney General or Director of National Intelligence need only provide to the court a sealed certification that five criteria are met, including the statement that a significant purpose of the surveillance is to obtain foreign intelligence

---

[30] *Id.* at 978. The author provides a detailed discussion and analysis of the Patriot Act's questionable relation with the Fourth Amendment.

[31] Abdolian, *supra* note 22, at 1429.

[32] *See* Robert F. Turner, *FISA vs. the Constitution*, THE WALL ST. J., Dec. 28, 2005, *available at* http://www.opinion journal.com/editorial/feature.html?id=110007734.

[33] *Id.*

[34] *Id.*

[35] *Id.*

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

[37] Fishman & McKenna, *supra* note 27, at § 1:12. *See also* The Protect America Act of 2007, *supra* note 36.

information.[38] The PAA also requires the Attorney General to report to Congress semi-annually on the number of certifications issued and any incidents of noncompliance with the PAA by an element of the intelligence community.[39]

Like the Patriot Act, the PAA was the subject of controversy for possibly violating American civil rights.[40] Nicknaming it the "Police America Act," the ACLU argued that under the PAA, the Attorney General alone, without oversight, has the authority to issue warrants for international surveillance for up to one year. The ACLU also argued that the Attorney General's reports to Congress were cursory and did not protect Americans against unnecessary surveillance.[41]

One defense of the PAA was propagated by the United States Department of Justice ("DOJ"). The DOJ argued that the PAA closed a critical gap in intelligence gathering by removing an obstacle to gathering foreign intelligence on targets located in foreign countries, and the DOJ stressed that the rights of persons located within the United States would continue to be protected.[42]

Another controversy arose from the Patriot Act and the PAA when the National Security Agency collected foreign intelligence information from telecommunications companies through an executive order. Several telecommunication companies cooperated with government officials by initiating wiretaps of private communications and other such surveillance during the period between September 11, 2001 and January 17, 2007.[43] The companies did not receive FISA orders to cooperate, but were told by government officials that the Attorney General had approved the program.[44] The controversy was whether these private corporations were actually authorized to provide assistance without a FISA order or other explicit

---

[38] Protect America Act of 2007 § 105(b).

[39] *Id.* at § 4.

[40] ACLU, *Analysis of the Protect America Act* (2007), http://www.aclu.org/national-security/aclu-analysis-protect-america-act (last visited April 13, 2010).

[41] *Id.*

[42] Department of Justice, *Dispelling the Myths*, http://www.justice.gov/archive/ll/paa-dispelling-myths.html (last visited April 13, 2010).

[43] *See* OFFICES OF INSPECTORS GENERAL, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 2 (2009), *available at* http://www.fas.org/irp/eprint/psp.pdf.

[44] *Id.* at 7.

authorization from the government. Because the PAA included an internal sunset provision, expiring on February 17, 2008, Congress had the opportunity to consider carefully the controversy as it was forced to reassess its position on foreign intelligence surveillance. [45]

The FISA Amendments Act of 2008 is the most recent update of FISA.[46] President Bush signed the amendments in July of 2008. He remarked on the legislation's critical role within the United States:

> The DNI and the Attorney General both report that, once enacted, this law will provide vital assistance to our intelligence officials in their work to thwart terrorist plots. This law will ensure that those companies whose assistance is necessary to protect the country will themselves be protected from lawsuits from past or future cooperation with the government. This law will protect the liberties of our citizens while maintaining the vital flow of intelligence.[47]

President George W. Bush was hopeful that the FISA Amendments Act of 2008 would bring about the resolution of the telecommunications controversy.

B. THE FISA AMENDMENTS ACT OF 2008

The FISA Amendments Act of 2008[48] amends FISA in order to establish a procedure for authorizing certain acquisitions of foreign

---

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

[46] For authorizations granted under the Protect America Act, §§105A, 105B, and 105C, continue to apply. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2472 (2008) [hereinafter FISA Amendments Act].

[47] The White House Office of the Press Secretary, Remarks by the President in Signing of H.R. 6304, FISA Amendments Act of 2008, July 10, 2008, http://www.justice.gov/archive/ll/docs/fisa-amendments-act-2008.pdf (last visited April 13, 2010).

[48] The FISA Amendments Act of 2008 was introduced as House Report 6304 on June 19, 2008, passed by the House of Representatives on June 20, 2008 and the Senate on July 9, 2008, and was signed into law by the President on July 10, 2008. It was passed in part to add an additional title to FISA allowing additional procedures for acquiring foreign communications. Govtrack.us, A Civic Project to Track Congress, http://www.govtrack.us/congress/billusc.xpd?bill=h110-6304 (last visited April 13, 2010).

intelligence and for other purposes.[49] There are two major impacts of the FISA Amendments Act of 2007: (1) it adds a title strictly to deal with the issue of surveillance on persons located outside of the United States, addressing the relevant provisions of the PAA in doing so, and (2) it provides immunity for the telecommunications companies that participated with government authorities in the past without having received a court order.[50] The third critical portion provides for a review of the President's post-September 11 authorized anti-terrorist surveillance.[51] The impact of this provision remains to be determined.

1. TITLE I: PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE U.S.

The first major change implemented by the FISA Amendments Act of 2008 is the addition of Title VII, entitled "Additional Procedures Regarding Certain Persons Outside the United States."[52] Partnered with this addition are the transition procedures for the PAA, which previously dealt with the issue of persons located outside the United States. The new section of FISA creates a framework for originating and conducting foreign intelligence surveillance of persons located outside the United States.[53]

Subject to certain limitations, the Attorney General and Director of National Intelligence ("DNI") have the authority to conduct surveillance of a non-United States person outside the United States for a period of up to one year.[54] This includes conducting wiretapping

---

[49] FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[50] *Id.*

[51] *Id.* The FISA Amendments Act of 2008 incorporates other provisions, but these three are deemed to be most relevant. A noteworthy provision not discussed in detail is the *en banc* authority the 2008 Act granted to the FISC. Upon its own initiative or upon request of the government, the FISC may hold a hearing (or rehearing) en banc when ordered by a majority of the judges if they determine that it is necessary to maintain uniformity of FISC decisions or if the particular proceeding involves a question of exceptional importance. *Id.* at § 109(b).

[52] *Id.* at § 101. Title I adds Title VII to FISA.

[53] *Id.* at Title I.

[54] *Id.* at §702(a). A United States person is defined by FISA as "a citizen of the United States, an alien lawfully admitted for permanent residence, . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in

operations within the United States of communications that both originate and terminate outside of the United States.[55]

There are two main differences between the PAA and the FISA Amendments Act of 2008. First, the PAA indicated that both the Attorney General and DNI have the authority to issue independent surveillance orders, while the FISA Amendments Act of 2008 states that the authority to provide surveillance orders must be exercised jointly.[56] Second, and more importantly, the 2008 Amendments Act provides limiting language on who can be targeted for surveillance where the PAA was silent. Under the Title VII jointly authorized surveillance orders, the target of surveillance cannot intentionally be a person known to be in the U.S. or a U.S. person reasonably believed to be located outside the United States.[57] A search pursuant to this joint authority cannot intentionally target a person reasonably believed to be outside the U.S. if the actual purpose of the surveillance is to target a known person reasonably believed to be within the borders of the United States.[58] Likewise, any communication where the sender and all recipients are known to be within the U.S. cannot be targeted by this type of surveillance.[59] While these precise limitations may or may not have been implicit in prior versions of FISA, the limitations are now the black letter law and serve to protect the rights and liberties of U.S. persons worldwide and of all persons located within the borders of the United States.

The FISA Amendments Act of 2008 also sought to resolve Fourth Amendment concerns raised by the original FISA and its progeny. The FISA Amendments Act of 2008 specifies that Title VII searches "shall be conducted in a manner consistent with the fourth amendment of the Constitution of the United States."[60]

While the DNI and Attorney General may not jointly authorize surveillance of a U.S. Person, Title VII of the FISA Amendments Act of

---

the United States . . . " Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(i).

[55] FISA Amendments Act, Pub. L. No. 110-261, § 702.

[56] *Id.*

[57] *Id.* at § 702(b).

[58] *Id.*

[59] *Id.*

[60] *Id.* at § 702(b)(5).

2008 does provide a method for conducting foreign intelligence surveillance of a U.S. person.[61] The U.S. person must be reasonably believed to be located outside the United States and, if the U.S. person is reasonably believed to be within the borders of the United States at any time, the surveillance must immediately cease.[62]

The FISC has jurisdiction to grant a FISA order allowing acquisitions inside the United States targeting a U.S. person reasonably believed to be located outside the United States to acquire foreign intelligence information "if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data."[63] The application for such a FISA order must meet several requirements; notably it must identify the U.S. person who will be the target and the facts relied upon to justify the applicant's belief that the U.S. person is reasonably believed to be outside the United States and is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.[64] The application must state that the significant purpose of the requested surveillance is to obtain foreign intelligence information and the requester must also include a statement of proposed minimization procedures.[65] In granting a FISA order based on this type of

---

[61] *Id.* at § 703(a)(1).

[62] *Id.* at § 703(a)(2).

[63] *Id.* at § 703(a)(1).

[64] *Id.* at § 703(b)(1). Foreign power is defined in the original FISA at §101(a), but the FISA Amendments Act of 2008 adds the following to the definition: "an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction." Likewise, "Agent of a Foreign Power" is also defined in the original FISA at §101(b), but the FISA Amendments Act of 2008 adds the following to the definition: "[a person who] engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power."

[65] *Id.* Minimization procedures are defined by the Act as: "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; notwithstanding paragraphs (1) and (2), procedures that allow for the retention and

application, the FISC must first find probable cause that the person is reasonably believed to be outside the U.S. and that the person is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power.[66] If the court finds that there is probable cause to believe these two criteria and other procedural requirements are met, the court can approve the targeting.[67] In determining probable cause, the judge is authorized to consider past activities of the proposed target, but the determination of whether the U.S. person is a foreign power or agent cannot be based solely upon activities protected by the First Amendment to the United States Constitution.[68]

Title VII of the FISA Amendments Act of 2008 provides the Attorney General with authority for emergency powers of surveillance. The Attorney General could authorize emergency surveillance against a U.S. person reasonably believed to be located outside the U.S. if a FISA order could be obtained, but could not be obtained in time to deal with the emergency foreign intelligence situation.[69] The Attorney General can only authorize this emergency surveillance acquisition if he or she (or a designee) informs a FISC judge at the time of the surveillance approval and subsequently files an application to the FISA court within seven days.[70] The emergency surveillance granted by the Attorney General expires within seven days of its approval or at the time the information sought is obtained, whichever happens first.[71]

---

dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802 (a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person." Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, § 101(h).

[66] FISA Amendments Act, Pub. L. No. 110-261, § 703(c)(1)(B).

[67] *Id.* at § 703(c)(1).

[68] *Id.* at § 703(c)(2).

[69] *Id.* at § 703(d).

[70] *Id.*

[71] *Id.* at § 703(d)(3).

Even though the PAA of 2007 expired in 2008, the transition procedures of the FISA Amendments Act of 2008 provided for the continued effect of FISA orders received pursuant to the PAA provisions for conducting foreign intelligence surveillance on persons located outside the United States.[72] Such orders will be given continued effect under the new legislation until it expires or final judgment is entered for any petition or litigation pending.[73] If the Attorney General or DNI wishes to continue or replace the PAA FISA order, they must adhere to the FISA Amendments Act of 2008 Title VII provisions.[74] The information gathered from surveillance approved under the PAA will be treated as if gathered under Title I of FISA as currently amended.[75]

The ACLU has voiced criticism of the FISA Amendments Act of 2008 with respect to the provision of Title VII.[76] Specifically, the ACLU claims that the FISA Amendments Act of 2008 permits the government to conduct surveillance of communications coming into and going out of the United States without any individualized review or finding of wrongdoing.[77] FISA, however, is not primarily a document for criminal investigation, but instead requires that the gathering of foreign intelligence information be a significant purpose of the investigation.[78] The finding of wrongdoing can be used under the FISA Amendments Act of 2008, but in order to initiate the investigation, the significant purpose must be national security.[79]

Conversely, others argue that the Act is *more* protective of privacy than its predecessors. Legal scholar Orin Kerr explains that the FISA Amendments Act of 2008 takes the basic approach of the PAA but

---

[72] *Id.* at § 404(a).

[73] *Id.*

[74] *Id.* at § 404(a)(7)(B).

[75] *Id.* at § 404(a)(3).

[76] ACLU, *Talking Points on the FISA Amendments Act of 2008*, http://www.aclu.org/national-security/talking-points-fisa-amendments-act-2008 (last visited April 13, 2010).

[77] *Id.*

[78] FISA Amendments Act, Pub. L. No. 110-261, §§ 702(g)(2)(A)(v), 703(b)(1)(F)(ii), 704(b)(5)(B).

[79] *Id.*

adds privacy protections and bolsters the scope of judicial review.[80] Responding to the PAA criticisms, he explained:

> On the whole, the new law strikes me as pretty good legislation: It nicely responds to the widely expressed fears last year about how the Protect America Act could be implemented and it ensures that the FISA Court will play a major role in reviewing surveillance of individuals located outside the U.S. Indeed, it seems to me that the new rules create pretty much the regime that critics of the Protect America Act wanted back in 2007.[81]

The FISA Amendments Act of 2008 does provide checks and balances on the authority of the Attorney General and DNI to initiate and continue to conduct foreign intelligence surveillance.[82]

Martin Lederman, former Department of Justice Attorney Advisor, suggests that there are aspects of the FISA Amendments Act of 2008 that are more protective of privacy than the earlier law because:

> [F]or the first time ever, surveillance of Americans *abroad* will require a court finding of probable cause to believe that the person is an agent of a foreign power. There is to be more congressional oversight. And, the new law requires the executive to adopt "minimization"

---

[80] Posting of Orin Kerr, Volokh Conspiracy, http://volokh.com/archives/archive_2008_07_06-2008_07_12.shtml#1215699055 (July 11, 2008, 2:38 AM). Orin Kerr is currently a law professor at The George Washington University Law School. Before joining the faculty, Professor Kerr was an Honors Program trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Department of Justice as well as a special assistant U.S. attorney for the Eastern District of Virginia. He also is a former law clerk for Judge Leonard I. Garth of the U.S. Court of Appeals for the Third Circuit and Justice Anthony M. Kennedy of the United States Supreme Court. *See* GW Law Faculty Profile, http://www.law.gwu.edu/Faculty/profile.aspx?id= 3568 (last visited April 13, 2010).

[81] Kerr Posting, *supra* note 80.

[82] FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

> procedures that comply with the traditional FISA minimization rules.[83]

While the ACLU continues to criticize foreign intelligence surveillance as currently authorized under FISA, the arguments that the FISA Amendments Act of 2008 serves to protect the civil rights and liberties of U.S. persons are extremely persuasive. Title VII to the FISA Amendments Act of 2008 illustrates that Congress sought to achieve the original goal of FISA by regulating foreign intelligence surveillance while preserving the rights of the American people.

2. TITLE II: ADDITION OF TITLE VIII: PROTECTION OF PERSONS ASSISTING THE GOVERNMENT

The second major change implemented by the FISA Amendments Act of 2008 as prescribed by Title II is the addition of Title VIII, entitled "Protection of Persons Assisting the Government."[84] Title VIII provides immunity for the electronic communication service providers that provide surveillance assistance to the intelligence community under very specific circumstances. In order to qualify for the immunity, the Attorney General must certify that one of three circumstances exists. First, the Attorney General must ensure that any assistance was provided pursuant to an order or directive under

---

[83] Posting of Martin Lederman, Balking Blogspot, http://balkin.blogspot.com/2008/07/privacy-protective-components-of-new.html (July 11, 2008, 8:21 AM). Martin Lederman is currently a law professor at the Georgetown University Law Center, and was an Attorney Advisor in the Department of Justice's Office of Legal Counsel from 1994 to 2002, where he concentrated on questions involving freedom of speech, the Religion Clauses, congressional power and federalism, equal protection, separation of powers, copyright, and food and drug law. Before that, he was an attorney at Bredhoff & Kaiser, where his practice consisted principally of federal litigation, including appeals, on behalf of labor unions, employees and pension funds, with particular emphasis on constitutional law, labor law, civil rights, RICO, and employment law. Most recently, he has been in private practice specializing in constitutional and appellate litigation. He regularly contributes to the weblogs "SCOTUSblog" and "Balkinization," including on matters relating to Executive power, detention, interrogation, and torture. He served as law clerk to then-Chief Judge Jack B. Weinstein, on the United States District Court for the Eastern District of New York, and to Judge Frank M. Coffin, on the United States Court of Appeals for the First Circuit. *See* Georgetown Law Full-Time Faculty Profile, http://www.law.georgetown.edu/faculty/facinfo/tab_faculty.cfm? Status= Faculty&ID=2134 (last visited April 13, 2010).

[84] FISA Amendments Act, Pub. L. No. 110-261, §201.

FISA.[85] Second, the Attorney General must ensure that the assistance was provided in connection with an intelligence activity authorized by the President between September 11, 2001 and January 17, 2007, which was designed to prevent or detect a terrorist attack against the United States.[86] This time-period encompasses what is known as the "President's Surveillance Program," discussed further below.[87] Finally, the Attorney General must ensure that the assistance was provided pursuant to a written request from the Attorney General or the head of an intelligence community to the provider, certifying that the activity was both lawful and authorized by the President.[88] If any one of the three criteria is satisfied, then no civil or federal action may be brought against an electronic communication service provider based upon its having provided information pursuant to the request.[89]

If the Attorney General certifies that one of the circumstances for surveillance exists, the FISC then reviews the circumstances, subject to one limitation:[90] If the Attorney General certifies that disclosure of the supplemental materials to be reviewed would harm national security, the FISC must review the materials *in camera* and ex parte.[91] The FISA Amendments Act of 2008 prohibits the states from conducting any investigation or implementing any regulation requiring disclosure of information about, or sanctioning, any electronic communication service providers for alleged assistance provided to any element of the intelligence community.[92] Title VIII ensures congressional oversight by requiring the Attorney General to report to certain congressional committees every six months.[93] The Attorney General is required to provide the committees with any certifications he has made and the judicial review of such

---

[85] *Id.* at § 802(a).

[86] *Id.*

[87] INSPECTORS GENERAL, *supra* note 43, at 1.

[88] FISA Amendments Act, Pub. L. No. 110-261, §802(a).

[89] *Id.* at § 802(a).

[90] *Id.* at § 802(b).

[91] *Id.* at § 802(c).

[92] *Id.* at § 803(a).

[93] *Id.* at § 804(a).

certifications, as well as any actions he has taken to ensure the states do not engage in any of the prohibited actions mentioned above.[94]

The Title VIII immunity provided for the telecommunications industry has generated great criticism. The debate begins when an electronic communication service provider is asked to cooperate with the government, and the question is whether that relationship is subject to the laws of the U.S. and judicial oversight of such legal compliance. While compliance with the laws of the U.S. is valued by parties on both sides of the debate, it is not agreed upon whether providing immunity for electronic communication service providers that turned over information to the government is a possible violation of such laws. If the cooperation between the telecommunications company and the government was in violation of the laws of the U.S., the debate is whether the company should be liable for its actions in court or whether the government should shield it from such liability because of the government's own involvement in the violation.

Attorney General certification and the resulting immunity under Title VIII of FISA as amended by the 2008 Act was found to be constitutional by the United States District Court for the Northern District of California in its recent decision *In re National Security Agency Telecommunications Records Litigation*.[95] The government intervened in a multidistrict litigation brought by individuals against telecommunications companies for alleged illegal wiretapping, moving for dismissal on FISA Amendments Act of 2008 Title VIII grounds.[96] The individuals responded by claiming that Title VIII was unconstitutional, using a series of arguments. The first was a separation of powers argument.[97] The individuals claimed that the executive branch forced the judicial branch to dismiss the cases without making an independent determination of facts upon which the dismissal was based.[98] The court held that while the judicial role may be small, it existed in the determination of whether or not the Attorney General's certification was proper and supported by

---

[94] *Id.* at § 804(b).

[95] *See* In re National Security Telecommunications Records Litigation, 633 F. Supp. 2d 949 (N.D. Cal. 2009). The court found that Title VIII did in fact create an "immunity" and not an affirmative defense, as some amici claimed.

[96] *Id.* at 955.

[97] *Id.* at 960.

[98] *Id.* at 961.

substantial evidence, and because the court was not directed to make specific findings, the separation of powers doctrine was not violated.[99] The individuals also raised a due process claim rejected by the court, as the court declared that Title VIII was constitutional and granted the government's motion to dismiss the action.[100]

As a presidential candidate, President Obama stated that he would try to strip the provision from the FISA Amendments Act of 2008, although he has since decided to support immunity.[101] The FISA Amendments Act of 2008 in its passage demonstrates that a majority of lawmakers agree that telecommunications industry immunity is best for the country. However, on September 17, 2009, Senator Russ Feingold introduced the Judicious Use of Surveillance Tools in Counterterrorism Efforts Act of 2009 ("JUSTICE Act"), which would remove the telecommunications corporations' immunity.[102] Senator Feingold claimed that the JUSTICE Act would protect American constitutional rights while preserving the government's powers to fight terrorism—a goal he shares with the FISA Amendments Act of 2008.[103]

3. TITLE III: REVIEW OF THE PRESIDENT'S SURVEILLANCE PROGRAM

The third major change implemented by the FISA Amendments Act of 2008 is provided in Title III, entitled "Review of Previous Actions."[104] Title III's review covers the "President's Surveillance Program." The term "President's Surveillance Program" refers to presidentially authorized intelligence activity involving communications from September 11, 2001 through January 17,

---

[99] *Id.* at 964. The individuals also further a non-delegation doctrine argument that the court after thorough analysis also rejects.

[100] *Id.* at 972.

[101] David S. Morgan, *Obama: I'll Fight To Strip Telecom Immunity From FISA*, CBS NEWS, June 21, 2008, *available at* http://www.cbsnews.com/blogs/2008/06/21/politics/horserace/entry4200105.shtml (last visited Feb. 28, 2010).

[102] Russ Feingold, Senators introduce Patriot Act Fixes to Safeguard Americans' Rights (September 17, 2009), *available at* http://feingold.senate.gov/record.cfm?id=317927 (last visited April 13, 2010).

[103] *Id.*

[104] FISA Amendments Act, Pub. L. No. 110-261, § 301.

2007.[105] Immediately following September 11, President George W. Bush authorized the National Security Agency ("NSA") to conduct a classified surveillance program in order to prevent further terrorist attacks, including the publicly disclosed "Terrorist Surveillance Program."[106] This program was the NSA's presidentially authorized interception of certain international communications where one party was a member of al-Qa'ida or a related terrorist organization.[107] Title III requires that all elements of the intelligence community who participated in this presidentially authorized intelligence activity complete a comprehensive review of their involvement in the program.[108] Specifically, each agency's inspector general must provide all facts concerning the establishment and implementation of the program and must describe the intelligence gathered and the agency's use of such intelligence.[109] Additionally, the inspector general must specify the participation of and communications with private individuals and entities.[110] The reports were to be consolidated and provided to certain congressional committees within one year of the Act's enactment.[111]

The long-awaited reports were issued in July 2009, but only portions were unclassified for review by the public.[112] The five inspectors general[113] produced a collective report that indicated

---

[105] *Id.* at § 301(a)(3).

[106] INSPECTORS GENERAL, *supra* note 43, at 1.

[107] *Id.*

[108] FISA Amendments Act, Pub. L. No. 110-261, § 301(b).

[109] *Id.*

[110] *Id.*

[111] *Id.* at § 301(c)(2).

[112] OFFICES OF INSPECTORS GENERAL, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, *supra* note 43, at Preface. The report provides an in depth discussion of the President's Surveillance Program. Further discussion of the contents are outside of the scope of this note.

[113] *Id.* The Inspectors General, who each submitted an individual report and then consolidated on a collective report, represent the following intelligence entities: the Department of Justice, the National Security Agency, the Central Intelligence Agency, the Department of Defense, and the Office of the Director of National Intelligence.

limited effectiveness of the program due to extreme secrecy.[114] The report did not assess whether the program violated FISA.[115] The FISA Amendments Act of 2008 does not specify what Congress is supposed to do with the reports upon receipt and what action will be taken next remains to be determined.

II. THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

In order to ensure FBI authority and flexibility in combating terrorism, Former Attorney General Michael Mukasey consolidated the guidelines for domestic FBI operations, effective December 1, 2008 (the "2008 Guidelines").[116] The FBI carries the primary role in conducting investigations within the United States for threats to national security.[117] The 2008 Guidelines establish the policy by which the FBI will achieve its directives while still respecting the liberty and privacy of the American people.[118]

A. THE 2008 GUIDELINES: BACKGROUND

The 2008 Guidelines were developed during President George W. Bush's administration, with the aim of protecting the United States against terrorism, expanding the FBI's intelligence gathering capability, bringing FBI domestic procedures to light, and

---

[114] *Id.* at 2-3.

[115] *Id.* at 3. The Officer of Professional Responsibility, however, has initiated a review of whether any professional conduct standards were violated in the preparation of legal memoranda in support of the President's Surveillance Program.

[116] *See* ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS, *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf (last visited April 13, 2010). The FBI is dedicated to its primary mission of protecting the United States from acts of terrorism by conducting surveillance and gathering intelligence. As the primary investigative agency of the federal government, the FBI investigates violations of federal law, national security threats, international terrorist threats, and conducts counterintelligence activities to deal with foreign espionage and intelligence efforts direct toward the United States. United States Department of Justice, Mission and Functions, *available at* http://www.justice.gov/nsd/mission_functions.htm (last visited April 13, 2010).

[117] ATT'Y GEN, *supra* note 116, at 5.

[118] *Id.*

"provid[ing] the American people with a firm assurance that the FBI is acting properly under the law."[119] The twin administrative goals of consolidation and bringing procedures to light were effectuated simply by publication in single procedural manual. Nevertheless, the substantive goals of protecting the U.S. against terrorism and expanding the FBI's intelligence gathering role are continuous and will be largely achieved through new assessment procedures.

Before the 2008 Guidelines, the FBI was operating under different manuals for different types of operations. The FBI honored the same wall between law enforcement and foreign intelligence investigations that existed under FISA in 1978. This created confusion as to which manual and set of procedures should be applied when a particular piece of information could be used for multiple purposes. In consolidating FBI domestic operations into one manual, the Attorney General replaced five separate manuals for FBI operations, providing a single, consistent structure that applies regardless of the type of information the FBI is seeking.[120]

The 2008 Guidelines were passed following recommendations by three advisory bodies: the National Commission on Terrorist Attacks Upon the United States ("9/11 Commission"), the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission"), and the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001 ("JIICATAS911").[121] In the years following the attacks of September 11, 2001, each of the advisory bodies made investigations, inquires, and inspections into the FBI to make necessary recommendations for the future of national security.

---

[119] *Id.*

[120] Department of Justice, *Fact Sheet: Attorney General Consolidated Guidelines for FBI Domestic Operations* (October 3, 2008), *available at* http://www.usdoj.gov/opa/pr/2008/October/08-ag-889.html. The new FBI guidelines repealed the following previous sets of guidelines: The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence, Attorney General's Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations, and The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest. ATT'Y GEN., *supra* note 116, at 14.

[121] *Id.*

All three advisory bodies agreed upon the role of the FBI and its best use in the future. The WMD Commission stated:

> [C]ontinuing coordination . . . is necessary to optimize the FBI's performance in both national security and criminal investigations. . . . [The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had on September 10, 2001.[122]

While consolidation is a goal, the main objective of the 2008 Guidelines is to emphasize early detection, intervention, and prevention of terrorist and criminal activities.[123] The FBI has long been transitioning into a proactive intelligence gathering body from its prior position as a more reactive body where agents waited to receive leads before acting. The 2008 Guidelines reflect the FBI's updated status as a "full-fledged intelligence agency and member of the U.S. Intelligence Community."[124]

The Obama Administration is continuing to implement the Guidelines, ensuring the FBI acts in accordance with the law. To assure the American people that civil rights are still being protected, the Obama Administration published that, "[a]s we grow our intelligence capabilities, the President is also committed to strengthening efforts to protect the privacy and civil rights of all Americans."[125]

The 2008 Guidelines general objective states:

---

[122] ATT'Y GEN., *supra* note 116, at 6.

[123] Department of Justice, *supra* note 120, at 6.

[124] *Id.*

[125] The White House, Issues: Homeland Security, http://www.whitehouse.gov/issues/homeland-security (last visited April 13, 2010).

> The full utilization of all authorities and investigative methods, consistent with the Constitution and the laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States."[126]

The FBI will achieve this objective through highly specified assessment procedures.

B. THE 2008 GUIDELINES: ASSESSMENTS

The 2008 Guidelines seek to expand the role of FBI intelligence by creating and implementing intelligence gathering protocols called "assessments." While not explicitly defined, the 2008 Guidelines describe assessments such that, "assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence."[127] According to the 2008 Guidelines, an assessment is the least intrusive investigation available and can be performed based on simple allegations or other information related to crimes or threats to national security.[128] Despite being less intrusive than other investigatory means, assessments still harbor much controversy.

The most controversial aspect of the 2008 Guidelines is the standard it sets for initiating an assessment. In order to initiate an assessment, there need only be a "proper purpose" and no "particular factual predication" is required.[129] The 2008 Guidelines thus allow limited investigation into an individual or group without a factual basis for the investigation. If there is an allegation, and the FBI's purpose is "proper," then the Bureau can perform an assessment.

To balance this low barrier to initiation, the 2008 Guidelines provide that assessments are to be conducted in a "manner of low intrusiveness," which the 2008 Guidelines define as gathering publicly

---

[126] ATT'Y GEN., *supra* note 116, at 5.

[127] *Id.* at 19.

[128] *Id.* at 18.

[129] *Id.* at 17.

available information via the government, Internet, or public or private entities.[130] The objective of an assessment can be simply detecting criminal activities, or it can be obtaining information about individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack by such activities.[131] Assessments can also be used to identify and assess individuals who may have value as human sources.[132]

Before the 2008 Guidelines created and implemented assessments, the FBI performed similar sounding "threat assessments."[133] Threat assessments were used "to investigate or collect information relating to threats to the national security, including information on individuals, groups, and organizations of possible investigative interests, and information concerning possible targets of international terrorism, espionage, foreign computer intrusion, or other threats to the national security."[134] Assessments as included in the 2008 Guidelines differ from the old threat assessments in that assessments are used for a broader range of activity, and can be conducted for additional purposes.[135] These purposes include:

---

[130] *Id.* at 20. The entire list of methods that can be used in an assessment are: obtain publicly available information, access and examine FBI and other Department of Justice records, and obtain information from FBI or any other Department of Justice personnel, access and examine any records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities, or agencies, use online services and resources (whether nonprofit or commercial), use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources, interview or request information from members of the public and private entities, accept information voluntarily provided by governmental or private entities, engage in observation or surveillance not requiring a court order, grand jury subpoenas for telephone or electronic mail subscriber information.

[131] *Id.* at 19.

[132] *Id.*

[133] ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES FOR NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION 12 (2003), http://www.fas.org/irp/agency/doj/fbi/nsiguidelines.pdf. This is one of the documents consolidated into the new FBI Guidelines; it created the category of "threat assessments."

[134] *Id.*

[135] ATT'Y GEN., *supra* note 116, at 19.

> Identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security; seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.[136]

The methods used in assessments are usually those methods available to the public; but because no factual predicate need exist, there is a danger that individuals will be the subject of an assessment based merely upon involvement in a group or religion.[137] Assessments under the 2008 Guidelines are highly controversial because they can be initiated without factual support. The general fear is that this will allow racial profiling and will limit freedom of association. The ACLU has criticized the 2008 Guidelines for, in the ACLU's view, "allowing a person's race or ethnic background to be used as a factor in opening an investigation."[138] This is a potential problem because an assessment can be initiated based only on an allegation and an approved proper purpose, which includes collecting information on groups of possible investigative interests.[139] The ACLU fears that the 2008 Guidelines fail to prevent the government from "infiltrating groups whose viewpoint it doesn't like."[140]

While the 2008 Guidelines do allow assessments based upon gathering information on groups of possible interest, there are

---

[136] *Id.*

[137] *Id.* at 17-18.

[138] *ACLU Condemns New FBI Guidelines* (Oct. 6, 2008), *available at* www.webwire.com/viewPressRel.asp?aId =76643 (last visited April 13, 2010).

[139] ATT'Y GEN., *supra* note 116, at 17.

[140] *ACLU, supra* note 138.

limitations built into the language that should protect the American people from racial or ethnic profiling. The first is that the gathering of information must be "relating to threats to the national security," and if the group does not participate in activities that relate to threats to the national security, they have no reason to fear "infiltration" by the FBI.[141] If there is a relation between the group and a threat to the national security, the FBI can initiate the assessment, but still must perform it in a manner of low intrusiveness as discussed above.

Moreover, in response to the criticisms mentioned above, former Attorney General Mukasey explained that the 2008 Guidelines would not alter the DOJ's rules that forbid predicating an investigation based solely on race, religion, or exercise of First Amendment rights.[142] The 2008 Guidelines specifically state: "these Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."[143]

While assessments cannot be initiated based simply on First Amendment activity, ethnicity, or race, the FBI can consider these factors if relevant. FBI General Counsel Valerie Caproni suggested that both race and religion can be significant factors in conducting an assessment, "especially where you are looking at a group where [ethnic or religious identity] is a membership criteria."[144] One such example is Hezbollah, of which almost all members are Lebanese Muslims; "if you have Lebanese Christians, you know you don't have a potential Hezbollah problem."[145]

The 2008 Guidelines were approved amid public outcry about their impact on civil rights, and they have been upheld by the current administration despite continued skepticism surrounding their

---

[141] ATT'Y GEN., *supra* note 116.

[142] Penny Starr, *New Intelligence Guidelines Encourage Racial Profiling, Dems Say*, CNSNEWS.COM, Sep. 12, 2008, http://www.cnsnews.com/news/article/35551.

[143] ATT'Y GEN., *supra* note 116, at 13.

[144] Andrew Kalloch, *FBI General Counsel defends new guidelines: Caproni Denies Use of Racial Profiling, Lauds F.B.I. as Domestic Intelligence Agency*, HARVARD LAW RECORD, Dec. 4, 2008, http://media.www.hlrecord.org/media/storage/paper609/news/2008/12/04/News/Fbi-General.Counsel.Defends.New.Guidelines-3568931.shtml.

[145] *Id.*

potential application.[146] Current Attorney General Eric Holder has not yet amended the 2008 Guidelines in any way, but has expressed interest in seeing how they work in operation. When asked by Senator Feingold about the 2008 Guidelines during his confirmation hearings, he stated: "[t]he guidelines are necessary because the FBI is changing its mission . . . from a pure investigative agency to one that deals with national security."[147]

CONCLUSION

The FISA Amendments Act of 2008 and the 2008 FBI Guidelines can be used by the current administration to increase intelligence capabilities while still protecting privacy and civil rights. When asked by Senator John Kyl about the FISA Amendments Act of 2008 at his confirmation hearing, Attorney General Eric Holder replied, "I believe that the law is constitutional . . . It's a very essential tool for us in fighting terrorism."[148]

The FISA Amendments Act of 2008 provides specific restrictions on the surveillance of persons located outside of the United States: the Attorney General and DNI must jointly authorize surveillance orders; U.S. persons outside of the continental U.S. are not to be targeted unless the FISC grants a FISA order based on probable cause that the person is both outside the U.S. and is actually an agent for a foreign power; and Attorney General-authorized emergency surveillance is only allowed if a FISC judge is notified immediately and it only lasts for seven days. It also protects the American people by prohibiting First Amendment activities from serving as the sole basis for the probable cause. The American people received a report on the President's Surveillance Program, with declassified portions for their review. The telecommunications immunity included in the FISA

---

[146] Eric Lichtblau, *New Guidelines Would Give F.B.I. Broader Powers*, N.Y. TIMES, Aug. 21, 2008 at A20, *available at* http://www.nytimes.com/2008/08/21/washington/21fbi.html. The author addresses some of the discussion surrounding the 2008 Guidelines before their passage, mentioning a letter sent by four democratic Senators to then-Attorney General Mukasey, saying that they fear the 2008 Guidelines "would allow the FBI to open an investigation of an American, conduct surveillance, pry into private records and take other investigative steps 'without any basis for suspicion.'"

[147] Nat Hentoff, *Is Eric Holder 'Change We Can Believe In'?*, JEWISH WORLD REVIEW, Feb. 18, 2009, *available at* http://www.jewishworldreview.com/cols/hentoff021809.php3?printer_friendly.

[148] *Id.*

Amendments Act of 2008 protects those who complied with the President's requests.

The 2008 Guidelines protect the American people by bringing FBI domestic policies to light. While initiating an assessment under the 2008 Guidelines may be easier than some prefer, assessments are conducted by gathering publicly available information that relates to threats to the national security. They also protect the American people by prohibiting the collection of information solely for the purpose on monitoring First Amendment activities.

The President has entrusted Attorney General Holder with preserving the delicate balance between conducting surveillance and protecting privacy and civil rights. In his opening speech at his confirmation hearing before the Senate Committee on the Judiciary, Holder proclaimed:

> If I have the honor of becoming Attorney General, I will pursue a very specific set of goals: First, I will work to strengthen the activities of the federal government that protect the American people from terrorism. Nothing I will do is more important. I will use every available tactic to defeat our adversaries, and I will do so within the letter and spirit of the Constitution.[149]

The 2008 Guidelines and the FISA Amendments Act of 2008 take steps to protect all within American borders. They do so by conducting surveillance activities in order to obtain intelligence necessary for our national security. They do so by protecting and preserving civil rights and privacy while conducting the surveillance.

---

[149] *Senate Confirmation Hearings: Eric Holder, Day One*, NY Times, January 16, 2009, *available at* http://www.nytimes.com/2009/01/16/us/politics/16text-holder.html?pagewanted=1.