NOTES

THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007

EMILY ARTHUR CARDY

INTRODUCTION

On December 16, 2005, the New York Times reported that the Bush administration authorized an alleged domestic spying program operated by the National Security Agency (NSA).[1] The President approved the program with a 2002 secret executive order.[2] Under the program, the NSA "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants . . . in an effort to track possible 'dirty numbers' linked to Al Qaeda."[3] The "Terrorist Surveillance Program" (TSP), as it came to be known, marked a dramatic shift in American intelligence-gathering because it permitted warrantless domestic spying.[4] Prior to the program, in general, "the government [could] only target phones and e-mail messages in the United States by first obtaining a court order from the Foreign Intelligence Surveillance Court."[5] In addition, prior to the TSP, the Federal Bureau of Investigation (FBI), rather than the NSA was re-

[1] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec.16, 2005, at A1.

[2] The 2002 Executive Order and the Terrorist Surveillance Program is classified; therefore, the Executive Order cannot be obtained. However, in addition to news outlets confirming that President Bush signed the Executive Order authorizing the program, President Bush himself stated that he authorized the program, though he did not state explicitly how he authorized it. President George W. Bush, President's Radio Address (Dec. 17, 2005) (transcript available at http://www.whitehouse.gov/news/releases/2005/12/20051217.html) (President Bush confirms that in "[i]n the weeks following the terrorist attacks on our nation, [he] authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations." and "This is a highly classified program that is crucial to our national security. Its purpose is to detect and prevent terrorist attacks against the United States, our friends and allies."); Risen & Lichtblau, *supra* note 1. Kelli Arena, *Bush Says He Signed NSA Wiretap Order*, CNN.com (Dec. 17, 2005), http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/index.html.

[3] Risen & Lichtblau, *supra* note 1.

[4] *Id.*

[5] *Id.*

sponsible for collecting domestic intelligence, including obtaining any necessary search warrants.[6] TSP shifted this responsibility from FBI to NSA.[7]

News of this significant policy change and its secretive authorization spread quickly as national media outlets reported on the program and Congress began an intractable debate both internally and with the Bush Administration.[8] Despite objections from Congress, the press, and the public, the Bush Administration refused to disclose details of the TSP's operation or its impact on Americans, citing the TSP's classified status.[9] The TSP eventually became the foundation for the Protect America Act of 2007 ("Protect America Act"), which effectively codified these warrantless domestic surveillance powers in the midst of public outcry and serious questions about the program's constitutionality.

Part II of this Note summarizes the enactment of the TSP as well as its connection to the Foreign Intelligence Surveillance Act (FISA), and provides a background for analyzing the Protect America Act's constitutional implications. Part III of this Note places the Protect America Act into political context, with an explanation of the Congressional debates and the Executive's role in the Act's passage. Part IV places the Protect America Act into legal context, with an explanation of relevant Fourth Amendment jurisprudence and an explanation of the Act's provisions. Part V argues that the Protect America Act permits unconstitutional, warrantless domestic spying powers, particularly through the word "concerning" in Section 2. Part V further argues that the Act fails to require adequate and independent evaluation of the intelligence activities it permits. Part VI discusses the Protect America Act's potential implications and discusses why, even if Congress repeals or amends the Act, its initial passage remains important. Although Congress eventually amended the Act, that initial August 2007 passage left Americans vulnerable to unconstitutional,

---

[6] *Id.* (before the TSP, the NSA conducted foreign surveillance with the exception of some surveillance on U.S. embassies and in Washington D.C. and New York City. The FBI, on the other hand, was responsible for domestic surveillance collection).

[7] *Id*.

[8] *See e.g.*, Dan Eggen, *Bush Authorized Domestic Spying; Post-9/11 Order Bypassed Special Court*, WASH. POST, Dec. 16, 2005, at A01; David G. Savage, *'78 Law Sought to Close Spy Loophole; Congress acted to prohibit the kind of domestic surveillance that is now at issue*, L.A. TIMES, Dec. 17, 2005, at A8; *Bush is taken to task on spying; Congress demands answers on NSA's eavesdropping in U.S.*, CHI. TRIB., Dec. 17, 2005, at 1; Ron Hutcheson, *Furor over revelations of spying; Specter vowed to probe the eavesdropping. Bush said the public and liberties were being protected.*, PHILA. INQUIRER, Dec. 17, 2005, at A01; Charlie Savage, *Senate Probe Report of US Spying; Furor on Surveillance Boosts Patriot Act Foes*, BOSTON GLOBE, Dec. 17, 2005, at A1; Suzanne Goldenberg, *Senate refuses to extend Patriot Act amid eavesdropping row*, THE GUARDIAN (LONDON), Dec. 17, 2005, at 15.

[9] Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, The White House (Dec. 19, 2005) (transcript available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html).

domestic surveillance and without remedy for such violations. Congress rubber-stamped the Bush Administration's plan, and in doing so Congress neglected its role as a check on executive power and tore from it's constituents a critical Constitutional protection.

PART II: LEGISLATIVE BACKGROUND

A. *Foreign Intelligence Surveillance Act*

In 1978 the Foreign Intelligence Surveillance Act (FISA) established the processes by which the United States intelligence community could effectively gather foreign intelligence, while striking "a balance between national security interests and civil liberties."[10] "FISA provides a means by which the government can obtain approval to conduct electronic surveillance of a foreign power or its agents without first meeting the more stringent standard" required in domestic criminal investigations.[11] That the TSP operated outside of FISA's purview made it automatically constitutionally suspect.[12]

The Article III court established by FISA, the Foreign Intelligence Surveillance Court (FISC), is essential to FISA's operation.[13] FISC objectively adjudicates intelligence collection proposals and procedures, while protecting such details in the interest of national security. In short, FISA establishes the United States' legal standard for gathering foreign intelligence, and provides safe-

---

[10] Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Attorneys, Cong. Research Serv., Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information 12 (Jan. 5, 2006); Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978). *See also* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2007).

[11] Memorandum from Bazan & Elsea, *supra* note 10, at 18.

[12] *See e.g.*, Curtis Bradley et al., *On NSA Spying: A Letter to Congress*, 53 N.Y. REV. OF BOOKS NO. 2 (Feb. 9, 2006), *available at* http://www.nybooks.com/articles/18650 (letter from fourteen American legal scholars and former government officials arguing that there is legitimate legal argument for the TSP); Letter from Curtis Bradley et al., to twelve Members of Congress, (Feb 2, 2006), http://www.law.yale.edu/documents/pdf/SecondNSA.pdf (second letter from the fourteen former government officials and legal scholars in response to the January 19, 2006 Department of Justice's "more extensive memorandum further explicating its defense for [the TSP]."); Press Release, American Civil Liberties Union, NSA Spying on Americans is Illegal (Dec. 29, 2005), http://www.aclu.org/privacy/spying/23279res2005 1229.html; Memorandum from Bazan & Elsea, *supra* note 10, at 42-43 (Though "[w]hether an NSA activity is permissible under the Fourth Amendment and the statutory scheme [for electronic surveillance] is impossible to determine without an understanding of the specific facts involved and the nature of the President's authorization, which are for the most part classified.").

[13] For discussion of FISA's status as a properly constituted Article III court, *see e.g.*, United States v. Cavanagh, 807 F.2d 787, 791-92 (9th Cir. 1987); U.S. v. Megahey, 553 F.Supp. 1180, 1196-98 (E.D.N.Y 1982).

guards to protect the Fourth Amendment's promises to the American public that they will be free from unwarranted government intrusion.[14]

The TSP operated outside of FISA and its safeguards, thus granting the intelligence community powers never sanctioned by Congress or Article III courts.

B. *The Bush Administration's Case for the TSP*

The Bush Administration argued that the President possesses the power to authorize the TSP through his inherent presidential power and through the 2001 Authorization for Use of Military Force in concert with the Supreme Court's *Hamdi v. Rumsfeld* decision.[15] The TSP's asserted purpose was to "detect and prevent terrorist attacks against the United States, our friends and allies"[16] by providing extra-FISA authority to more quickly collect certain kinds of intelligence.[17] Specifically, the TSP argued that changes in technology since FISA's passage unintentionally expanded FISA's coverage to include intelligence collection Congress never intended, meaning that the government had to obtain a warrant to collect "intelligence information against a target located overseas,"[18] which was not FISA's intent. The Administration claimed that requiring a court order to "conduct surveillance on foreign intelligence targets located in foreign countries"[19] would unnecessarily hamper the intelligence community's ability to collect accurate and timely information.[20] Yet, in defending the TSP, the Administration failed to address the program's primary constitutional problem: in addition to providing for legitimate foreign surveillance, the TSP also permitted warrantless domestic spying, a key feature that later remained in the Protect America Act.

---

[14] Memorandum from Bazan & Elsea, *supra* note 10. Executive Order 1233 passed on December 4, 1981 is also a critical piece in United States foreign intelligence law, but this note focuses only on the Protect America Act's relationship to FISA, and not to Executive Order 12333. Exec. Order No.12333, 46 Fed. Reg. 59,942 (Dec. 4, 1981), *as amended by* 50 U.S.C. § 401 (1947).

[15] Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Memorandum from Bazan & Elsea, *supra* note 10, at 27-36 (commenting on Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001)). *See also*, Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, *supra* note 9; Press Release, The White House, President George W. Bush, Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program (Jan. 22, 2006), http://www.whitehouse.gov/news/releases/2006/01/20060122.html.

[16] President George W. Bush, President's Radio Address, *supra* note 2.

[17] Press Briefing, Attorney General Alberto Gonzales and General Michael Hayden, *supra* note 9.

[18] Press Release, The White House, President George W. Bush, Fact Sheet: The Protect America Act of 2007 (Aug. 6, 2007), http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html.

[19] *Id*.

[20] *Id.*

C. *Congressional Action*

At the urging of the Bush Administration, particularly of Mike McConnell, the Director of National Intelligence, in the spring of 2007 Congress began considering codifying TSP (which would later become the Protect America Act). The Administration urged Congress to "modernize" FISA to keep step with technological advances since FISA's passage in 1978.[21] In short, the Administration sought to codify the TSP, and Congress began considering incorporating TSP into FISA.

Congress reached a consensus on the eve of its August 2007 recess, approving the Protect America Act of 2007; on August 5, 2007, President Bush signed the bill into law.[22] The Act amended FISA to include intelligence collection procedures similar to, but arguably broader than those permitted by the TSP.[23] Instead of continuing to oppose an NSA-style program like the TSP, Congress sanctioned it. However, that Congress and the President approved the Act does not guarantee that it is constitutional. The Protect America Act's far-reaching provisions permit unconstitutional surveillance of United States citizens, implicating the Fourth Amendment. In some ways the Protect America Act is more constitutionally troubling than was the TSP. Whereas the secretly-established TSP over-extended Executive power, the Protect America Act was passed by a transparent legislative process, and permits unconstitutional domestic surveillance.

PART III. POLITICAL BACKGROUND OF THE PROTECT AMERICA ACT

When President Bush signed the Protect America Act on August 5, 2007, the U.S. government essentially codified the previously extra-legal TSP. This codification, however, does not lend the activities sanctioned in TSP and in the Protect America Act enough legitimacy to overcome their unconstitutionality.[24]

A. *Executive Action*

On April 13, 2007, the Bush Administration submitted a request to Congress for "long overdue changes to FISA," the asserted purpose of which was to "bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interest

---

[21] Press Release, The White House, President George W. Bush, *supra* note 18; BAZAN, *supra* note 10, at 1. *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, CONG. RESEARCH SERV., Report for Congress RL34143 1 (Aug. 23, 2007).

[22] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified at 50 U.S.C §§ 1805(a)-(c), 1803 note).

[23] *See* 153 CONG. REC. S10866 (daily ed. Aug. 3, 2007) (statement of Sen. Feingold). *See also infra* Part IV.B.

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

of persons located in the United States."[25] Presumably this attempt at codifying the TSP resulted from pressure directed at the Administration for operating the TSP outside of FISA and without Congressional approval. By August 2007, Mike McConnell, submitted a modified version of the April 2007 legislative request.[26] The Senate Select Committee on Intelligence held open hearings on the FISA amendments on May 1, 2007.[27] Both the Bush Administration's request and the Senate committee's hearing opened the door wider for immediate Congressional action: the request was leaner, and Congress had yet to tackle the purportedly critical FISA amendment before the looming August recess.

McConnell testified in support of the legislative request,[28] testifying before the Senate Select Committee on Intelligence on May 1, 2007, and making a statement to Congress on August 2, 2007.[29] His August 2, 2007 statement outlined the Administration's intelligence requests and created a sense of urgency for Congressional action.[30] McConnell emphasized that "we must urgently close the gap in our current ability to effectively collect foreign intelligence. The current FISA law does not allow us to be effective."[31] McConnell's statement called for three key changes to the existing law: First, "the [i]ntelligence [c]ommunity should not be required to obtain court orders to effectively collect foreign intelligence from foreign targets located overseas."[32] Second, and more importantly, "the [i]ntelligence [c]ommunity should not be restricted to effective collection of only certain categories of foreign intelligence when the targets are located overseas."[33] Third, McConnell requested that the law not require the intelligence community to obtain court approval "before urgently needed intelligence collection can begin against a foreign target located overseas."[34] He did, however, concede that the Administration would accept a re-

---

[25] Press release, Department of Justice, Office of the Director of National Intelligence, Fact Sheet: Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act (Apr. 13, 2007), http://www.dni.gov/press_releases/20070413_release.pdf.

[26] Letter from J. Michael McConnell, Director of National Intelligence to Honorable John D. Rockefeller, Chairman, Senate Select Committee on Intelligence and Honorable Christopher S. Bond, Vice Chairman, Senate Select Committee on Intelligence (April 27, 2007).

[27] *Modernization of the Foreign Intelligence Surveillance Act, Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 1 (2007).

[28] *Id.* at 7-22 (statement of Mike McConnell, Director of National Intelligence); Press Release, Director of National Intelligence, Modernization of the Foreign Intelligence Surveillance Act (FISA) (August 2, 2007), http://www.dni.gov/press_releases/20070802_release.pdf.

[29] *Id.*

[30] Press Release, Director of National Intelligence, *supra* note 28.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

quirement mandating court approval after the collection process began.[35]

McConnell stressed that requiring court review before collecting information would hamper intelligence gathering where critical national security interests were at stake.[36] Implicit in his statement was the belief that agencies should be permitted to gather some intelligence without restriction—so long as the person *about* whom the government collected information was outside of the United States, the method for gathering such information mattered little. McConnell's testimony heavily influenced subsequent Congressional debate and eventual passage of the bill, which implicates questions of improper Executive influence on Congress' legislative function.[37] McConnell's proposal, outlined on August 2, 2007 was essentially the same as Senate Bill 1927. A few days later the Senate bill was passed as Public Law 110-55, the Protect America Act of 2007.[38]

B. *Congressional Action*

The Protect America Act moved through Congress remarkably quickly, particularly given the magnitude of changes the Act implemented. From the date of introduction into Congress, to the bill's signing, the Act's entire legislative process, which often requires months or years, spanned only five days.[39] On August 1, 2007, Senator Mitch McConnell introduced Senate Bill 1927, which would eventually become the Protect America Act.[40] On August 3, 2007, Senator Carl Levin and Senator John D. Rockefeller introduced Senate Bill 2011, a

---

[35] *Id.*

[36] *Id.*

[37] *See e.g.*, 153 CONG. REC. S10863 (daily ed. Aug. 3, 2007) (statement of Sen. Kit Bond, a co-sponsor of the bill that eventually passed) ("I invite [my colleagues] to . . . talk directly with Admiral McConnell [Director of National Intelligence] because I think it is extremely important that you find out what his position truly is."); 153 CONG. REC. S10863 (daily ed. Aug. 3, 2007) (statement of Sen. Harry Reid) ("I am concerned that we have Admiral McConnell here checking on us. . . . I think it is wrong that this man whom we put in a very important position is here roaming the halls finding out how we are going to vote . . . .") (implying that the implicit pressure from a member of the Executive was inappropriate.); 153 CONG. REC. S10864 (daily ed. Aug. 3, 2007) (statement of Sen. Russ Feingold) ("The day we start deferring to someone who is not an elected Member of this body, or hiding behind him when you do not have the arguments to justify your position is a sad day for the Senate."); 153 CONG. REC. S10865 (daily ed. Aug. 3, 2007) (statement of Sen. Russ Feingold) ("In times of war, we don't give up our responsibility in the Senate to review and make laws. The notion that we simply defer this to the Director of National Intelligence and whatever he says is an abdication of our duties, especially in times of war."). While this goes beyond this Note's purview, the Director of National Intelligence's role in the legislative process may highlight questions of separation of powers regarding the Executive's proper role in a historically and constitutionally legislative function.

[38] *Id.*

[39] 110 Bill Tracking S. 1927 (LEXIS).

[40] *Id.*

more moderate version, which failed passage by a 43-45 partisan vote.[41] Senate Bill 1927 bypassed committee and was automatically placed before the full Senate (Committee of the Whole) for debate and consideration.[42] The Senate debated and passed the bill on August 3, 2007, and sent it to the House of Representatives for consideration.[43] The House debated and passed the Protect America Act with no amendments the following day, August 4, 2007, despite the fact that they had debated H.R. 3356, a different version of Senate Bill 1927 only a day before.[44] Passing Senate Bill 1927 without amendment permitted circumvention of the conference committee process, resulting in greater expediency. On August 5, 2007 the President signed into law the Protect America Act of 2007.[45] Senator Mitch McConnell included a sunset provision, which required Congress to take up the issue again in six months (this provision was the only other legislative action to occur during the bill's legislative process).[46]

Despite the Act's swift passage through Congress, Senate debate demonstrated that senators were aware of the bill's powerful and potentially nefarious implications. For example, Senator Reid stated:

> It authorizes, in my opinion, warrantless searches of Americans' phone calls, e-mails, homes, offices and personal records . . . . [T]he search does not have to be directed abroad, just *concerning* a person abroad . . . any search inside the United States [which] the Government can claim to be concerning al-Qaida is authorized. I do not believe that is the right way . . . or the Constitutional way to fight the war on terrorism.[47]

Senator Feingold echoed his concerns:

> [T]his bill would go way too far. It would permit the Government, with no court oversight whatsoever, to intercept the communications of calls to and from the United States, as long as it is directed at a person—any person, not a suspected terrorist—reasonably believed to be outside the United States.[48]

Senator Feingold added that, in fact, the provisions of this bill went beyond those TSP provisions that the Administration made public.[49]

Throughout the debate, when critics argued that the bill provided too much

---

[41] 110 Bill Tracking S. 2011 (LEXIS). *See generally* S. 2011, 110th Cong. (2007).

[42] 110 Bill Tracking S. 1927 (LEXIS).

[43] *Id.*

[44] *Id*; 110 Bill Tracking H.R. 3356 (LEXIS). *See generally* H.R. 3356, 110th Cong. (2007).

[45] 110 Bill Tracking S. 1927 (LEXIS).

[46] Protect America Act of 2007, Pub. L. No. 110-55, § 6(c), 121 Stat. 552, 557; 110 Bill Tracking S. 1927 (2007).

[47] 153 CONG. REC. S10864 (daily ed. Aug. 3, 2007) (statement of Sen. Harry Reid) (emphasis added).

[48] 153 CONG. REC. S10866 (daily ed. Aug. 3, 2007) (statement of Sen. Russ Feingold).

[49] *Id.*

power with too little oversight, proponents offered one response—that the bill provided the intelligence community with information necessary to secure the nation against terrorism.[50] However, during the Senate debates, the bill's supporters never refuted the proposition that Senate Bill 1927 (later the Protect America Act) could authorize warrantless domestic surveillance.[51]

Additionally, bill supporters continually emphasized that the Director of National Intelligence preferred the Senate Bill 1927, and that it was the only version of the bill the President would sign.[52] The extreme deference paid to the Executive during these debates indicates that Congress abdicated its responsibility to act as a check on Executive power. In allowing the Executive to lead the Protect America Act's legislative process, Congress also abdicated its responsibility to act as the sole national legislative body. This failure is illustrated by the Director of National Intelligence's presence outside of the Senate chamber during the bill's consideration – an occurrence which excited comments by numerous senators.[53] The Director remained immediately outside of the chamber to provide Senators ample opportunity to speak with him about the Administration's aspirations for the legislation.[54] In fact, Senator Bond specifically invited his colleagues to speak with the Director of National intelligence "to find out what his position truly is," which Bond found critically important in deciding how to vote.[55] Lastly, the Protect America Act debate occurred immediately before Congress's August recess. The debate's timing exerted additional pressure on the legislative process, potentially producing legislation that would not otherwise have passed.[56]

Senate Bill 1927's sunset provision became a legislative crutch because it required that Congress review the legislation six months after it passed.[57] Several senators remarked that the sunset provision was reason to pass the legisla-

---

[50] 153 CONG. REC. S10865 (daily ed. Aug. 3, 2007) (statement of Sen. Joseph Lieberman) ("These are our soldiers in the war against terrorism. I want to give them the power and authority they need to find out what our enemy is doing so we can stop them before they attack us.").

[51] *See generally* 153 CONG. REC. S10861-73 (daily ed. Aug. 3, 2007).

[52] *See e.g.*, 153 CONG. REC. S10869 (daily ed. Aug. 3, 2007) (statement of Sen. Arlen Specter).

[53] *See generally* 153 CONG. REC. S10861-73 (daily ed. Aug. 3, 2007).

[54] *Id.*

[55] 153 CONG. REC. S10863 (daily ed. Aug. 3, 2007) (statement of Sen. Kit Bond).

[56] *See e.g.*, 153 CONG. REC. S10865 (daily ed. Aug. 3, 2007) (statement of Sen. Joseph Lieberman) ("[L]et us not strive for perfection. Let us put national security first. Let us understand if this passes, as I pray it will, and the President signs it, as I know he will if it passes both Houses, we are going to have 6 months to reason together to find something better."); 153 CONG. REC. S10866 (daily ed. Aug. 3, 2007) (statement of Sen. Russ Feingold) ("I am concerned that we are moving too fast and that we have not necessarily come up with the right answer to the problem we all recognize exists.").

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

tion because it forced Congress to reconsider the legislation and allow them to change it.[58] This attitude overlooked the fact that reviewing the legislation six months later would not prevent constitutional violations during the interim six months and would do nothing to vindicate people's constitutional rights which the Act compromised. The combination of the August recess, Executive interference, McConnell's presence, and the sunset clause created a culture of diffused responsibility for passing the Act. Congress did not hold open hearings about the Protect America Act until September 25, 2007, almost two months after President Bush signed it into law.[59] Consequently, in part because of the crutch provided by the sunset provision, Congress passed the legislation – understanding but disregarding its serious implications.[60]

C. *Presidential Action*

President Bush released three brief statements about the Act: two on August 4, 2007 and one on August 5, 2007.[61] The White House also released a Protect America Act of 2007 fact sheet on August 6, 2007.[62] However, the President did not issue a signing statement and the President's weekly digest did not contain information about the Act's signing.[63] The brief August 4th statements recognized the Senate's and the House's passage of the Act and urged that, until the Act was permanent, the work on closing the FISA gaps was incomplete.[64] The August 5th statement commended Congress for passing the Protect America Act, hailed the legislation's benefits, including claims about protecting civil liberties, and urged further Congressional action after the August re-

---

[58] *See generally* 153 CONG. REC. S10861-73 (daily ed. Aug. 3, 2007).

[59] *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (Sept. 25, 2007) (including testimony by Mike McConnell, Director of National Intelligence).

[60] *Id.* The Protect America Act may have been discussed during closed Senate Intelligence Committee hearings, but the topics of closed hearings are not available to the author. The Senate Select Committee on Intelligence held twelve closed hearings between the passage of the Protect America Act by the Senate on August 3, 2007and the Senate Committee on the Judiciary hearing on September 25, 2007. *See* Hearing Schedule, Senate Select Committee on Intelligence, http://intelligence.senate.gov/hearings.cfm.

[61] Statement on Senate Passage of Intelligence Reform Legislation, 43 WEEKLY COMP. PRES. DOC. 1047-48 (Aug. 13, 2007); Statement on House of Representatives Passage of Intelligence Reform Legislation, 43 WEEKLY COMP. PRES. DOC. 1048 (Aug. 13, 2007); Statement on Congressional Passage of Intelligence Reform Legislation, 43 WEEKLY COMP. PRES. DOC. 1048-49 (Aug. 13, 2007).

[62] Press Release, The White House, *supra* note 18.

[63] Statements by the President, 43 WEEKLY COMP. PRES. DOC. 1047-70 (Aug. 13, 2007).

[64] Statement on Senate Passage of Intelligence Reform Legislation, *supra* note 61; Statement on House of Representatives Passage of Intelligence Reform Legislation, *supra* note 61.

cess.[65] The statement further celebrates the Act's bi-partisan passage and characterizes it as modernizing FISA and closing loopholes in the law.[66] It characterizes FISA as having "not kept pace with revolutionary changes in technology" and as a result, American "intelligence professionals have told us that they are missing significant intelligence information that they need to protect the country."[67] The President's statement continues, stating that the Protect America Act "gives our intelligence professionals this greater flexibility while closing a dangerous gap in our intelligence gathering activities that threatened to weaken our defenses."[68] This elevated rhetoric contrasts sharply with the dearth of public communication about the Act and lack of fanfare surrounding its passage.[69]

PART IV: LEGAL BACKGROUND OF THE PROTECT AMERICA ACT

As Public Law 110-55, the Protect America Act is codified within and amends FISA section 105.[70] Although being a part of FISA could seem to lend legitimacy to the Act, it does not, because FISA's safeguards do not extend to the Act.[71] The Protect America Act explicitly situates its provisions outside of FISA and outside of FISC's purview. While hailed as a success in forcing the Administration to codify and bring the TSP into FISA, the Protect America Act actually provides broader executive power than the original TSP, and places the program substantially outside of the United States' legal standard governing intelligence collection. The provisions in the Protect America Act permit activities in contravention of Fourth Amendment jurisprudence.

A. *The Fourth Amendment*

The Fourth Amendment of the United States Constitution, and the common law jurisprudence interpreting it, provide the current body of law regulating domestic search and seizure, including domestic electronic surveillance. The Fourth Amendment protects Americans from unreasonable searches and seizures by requiring probable cause and particularity for a search warrant (which then makes the search reasonable), and requiring a search warrant except in exceptional circumstances.[72]

---

[65] Statement on Congressional Passage of Intelligence Reform Legislation, *supra* note 61.

[66] *Id.* at 1048.

[67] *Id.*

[68] *Id.*

[69] *See Id.*

[70] Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552.

[71] *See infra* Part IV.B.

[72] U.S. CONST. amend. IV. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized."

Though Fourth Amendment jurisprudence originally applied only to tangible things, the Supreme Court eventually extended the Fourth Amendment's reach to include conversations; and the Court continued this expansion as technology advanced.[73] In *Katz v. United States*, the Supreme Court held "for the first time that the protections of the Fourth Amendment extend to circumstances involving electronic surveillance of oral communications without physical intrusion."[74] *Katz* was groundbreaking because it overruled an earlier case, *Olmstead v. United States,* which held that the Fourth Amendment did not apply to wiretapping phone conversations because words were intangible, and, therefore, no search and/or seizure had occurred.[75] Because *Katz* established that the Fourth Amendment applies to electronic surveillance activities, and the Protect America Act permits warrantless domestic surveillance through electronic communication, the Act implicates the Fourth Amendment.

Five years after *Katz*, the Supreme Court addressed electronic surveillance for domestic intelligence purposes in *United States v. United States District Court* (known as *Keith*).[76] The Court extended *Katz's* holding when it found that "the President violated the Fourth Amendment by authorizing warrantless wiretaps in national security cases."[77] Boston University School of Law Professor Tracey Maclin notes:

> Powell's reasoning [in *Keith*] was succinct and categorical: The warrant requirement applied to national security wiretaps and there was no basis for exempting the President from the requirement. There was no nuance and no room for manipulation by the government.[78]

Additionally, *Keith* made clear that the warrant requirement applies even when the Executive believes national security is at risk.[79] The court recognized the President's constitutional duty to protect national security with the caveat that "it must be exercised in a manner compatible with the Fourth Amendment."[80] Thus, while the *Keith* decision did not express a view on "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country,"[81] it firmly established that warrantless domestic surveillance is constitutionally impermissible even in the name of na-

---

[73] Memorandum from Bazan & Elsea, *supra* note 10, at 8.

[74] *Id*. (citing Katz v. United States, 389 U.S. 347, 359 n.23 (1967)).

[75] Olmstead v. United States, 277 U.S. 438, 464-466 (1928).

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

[77] Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case,* 41 U.C. DAVIS L. REV. 1259, 1263-4 (2008).

[78] *Id.* at 1265.

[79] *Id.* at 1266-67.

[80] *Keith*, 407 U.S. at 320.

[81] *Id.* at 308.

tional security.[82]

B. *The Protect America Act's Provisions*

The Protect America Act is FISA section 105. It also amended parts of section 103, and is therefore also codified within the United States Code as 50 U.S.C. Sections 1805 and amended parts of Section 1803.[83] For the purposes of clarity, when referring to FISA sections that are not part of the Protect America Act, this note will reference the FISA sections themselves (ex. 101, 102, 103, etc.) and not the corresponding United States Code sections (1801, 1802, etc). Also, this note will reference Protect America Act sections written as free-standing public law (ex. section 2(a)(2)) and not the corresponding FISA or United States Code sections. The Protect America Act's critical sections are sections 2, 3, 4, and 6.

1. Foreign Intelligence Defined

The definition of "foreign intelligence" is critical to the constitutional analysis of the Protect America Act. The Act does not provide a different definition of "foreign intelligence" from the one provided in FISA; thus in interpreting the Protect America Act, FISA's definition of "foreign intelligence" applies.[84] In FISA's definition, "foreign" applies to the *content* of the information gathered, and not to the location in (or from) which the information is gathered, or the nationality of the sources from which it is gathered.[85] Instead, "foreign intelligence" means "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . " harms or clandestine operations against the United States.[86] The definition

---

[82] Memorandum from Bazan & Elsea, *supra* note 10, at 10. The Court also "invited Congress to establish statutory guidelines" with respect to surveillance involving foreign powers and their agents. *Id*. at 10.

[83] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified at 50 U.S.C. §§ 1805(a)-(c), 1803 note).

[84] Foreign Intelligence Surveillance Act (FISA) § 101(e), 50 U.S.C. § 1801(e) (2006).

[85] *Id.*

[86] *Id.* The full FISA definition of "foreign intelligence information" is as follows: "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

does not contain any language limiting the country from which the information may be collected.[87] Thus, while the Act's asserted purpose is to collect *foreign intelligence*, the Act's definition of foreign intelligence does not provide inherent protection against domestic surveillance – domestic surveillance is not precluded from the definition of foreign surveillance. How an act defines its terms, rather than the terms themselves out of context, dictates the Act's application; this is a critical point in understanding the Protect America Act's far-reaching implications.

2. Redefining "Electronic Surveillance"

The Protect America Act redefines electronic surveillance, despite the fact that FISA's definition of foreign surveillance continues to apply. Section 2 of the Protect America Act provides the law's "first substantive provisions."[88] First, Section 2 establishes that the FISA definition for electronic surveillance, section 101(f),[89] does not apply to the activities described in the Protect America Act.[90] FISA's definition of electronic surveillance contains clauses relating to the target and the collection procedures defined as "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication."[91] In rejecting this definition, the Protect America Act states that "nothing in the definition of electronic surveillance under section 101(f) [of FISA] shall be construed to encompass surveillance directed at a

---

(B) the conduct of the foreign affairs of the United States."

87 *Id.*

88 BAZAN, *supra* note 10, at 2.

89 FISA § 101(f) defines electronic surveillance as the following:

(1) 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, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) 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 in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) 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, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

90 Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552.

91 FISA § 101(f).

person reasonably believed to be located outside of the United States."[92] Therefore, if surveillance is directed at a person "reasonably believed to be outside the United States," FISA's definition of electronic surveillance does not apply to that intelligence gathering, because it is a Protect America Act collection, not a standard FISA collection. Such person does not benefit from FISA's protections or the limitations FISA places on intelligence collection; instead the Protect America Act governs the activities directed at that person.

Additionally, section 2 does not explicitly state that this exception to FISA's electronic surveillance definition applies only to surveillance of a foreign person.[93] It also does not "explicitly address the location of the parties to the communication or the location of the acquisition of the information involved."[94] The meaning of "directed at" could therefore permit surveillance of individuals other than the target[95] in order to gain information about that foreign target. Because FISA section 101(f) does not limit the Protect America Act, the people from whom the intelligence community gathers information about the target could include people inside the United States and/or United States citizens.[96] Congress defined the activities in the Protect America Act as outside FISA's meaning of "electronic surveillance,"[97] thereby excluding those activities from the limitations placed on "electronic surveillance" by FISA, such as warrants or court approval.[98]

Section 102 of FISA provides limitations on when and how warrantless electronic surveillance may be conducted. But, because Section 2 of the Protect America Act defines its activities as *not* constituting electronic surveillance under FISA, these protective requirements do not apply to the activities permitted by the Protect America Act.[99] Section 102 provides that the President can authorize warrantless electronic surveillance "to acquire foreign intelligence information" for up to one year, provided that certain conditions are met.[100] The Attorney General must certify that the surveillance is "solely directed at" a specific target, acquires communications "exclusively between or among foreign powers," lacks a "substantial likelihood that the surveillance will acquire. . .any communication to which a United States person is a party," and uses appropriate minimization procedures.[101] These procedures provide greater

---

[92] Protect America Act § 2.

[93] *Id.*

[94] BAZAN, *supra* note 10, at 5.

[95] The word "target" references the individual(s) about which the intelligence community is collecting information.

[96] Protect America Act § 2; BAZAN, *supra* note 10, at 3-5.

[97] Protect America Act § 2.

[98] FISA §§ 102-104 (providing the guidelines for gaining FISA court approval for electronic surveillance and for enabling electronic surveillance without a court order).

[99] FISA § 102(a)(1).

[100] *Id*.

[101] *Id*.

protections against domestic surveillance than do the Protect America Act's provisions. The Protect America Act's collection procedures and protective requirements grant intelligence officials greater discretion and generally provide fewer protections for individuals than do FISA's provisions.

3. Intelligence Collection Procedures

While the first part of Protect America Act's section 2 describes what procedures do not apply to it, section 2(a) begins by describing the procedures it controls.[102] Section 2(a) provides the procedure for collecting "acquisitions concerning persons located outside the United States," and provides an alternative to FISA's method for the President to acquire "foreign" intelligence without a warrant.[103] Additionally, the language "notwithstanding any other law" in this section indicates that the procedures outlined in the Act supersede any existing law that might have applied.[104]

Unlike FISA's Section 102, which provides limitations on warrantless electronic surveillance, the Protect America Act's section 2(a) does not limit warrantless information acquisition, even if there is a substantial likelihood that a party to the surveyed communication is either a United States citizen, or an individual located within the United States.[105] Instead, section 2(a) allows the President to authorize warrantless collection of foreign intelligence for up to one year, provided that:[106]

1. "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States;"[107]
2. "the acquisition does not constitute electronic surveillance;"[108]
3. "the acquisition involves obtaining the foreign intelligence information from or with the assistance of communications service provider, custodian, or other person. . .who has access to communications;"[109]
4. "a significant purpose of the acquisition is to obtain foreign intelligence information;"[110] and

---

[102] Protect America Act § 2(a).

[103] *Id.* (note again that this section does not use the word "surveillance," since FISA §105A defined the activities described in §105B as not being electronic surveillance.)

[104] *Id.* § 2(a).

[105] *Id.*

[106] *Id*.

[107] *Id*. § 2(a)(1).

[108] However, the Act does not specify how the definition must differ from FISA's electronic surveillance definition, other than complying with the Protect America Act, which explicitly says that nothing in it is to be construed as being "electronic surveillance." *Id.* § 2(a)(2).

[109] *Id.* § 2(a)(3).

[110] *Id.* § 2(a)(4).

5. FISA Section 101(h) minimization procedures are followed.[111]

Section 2(a), understood in conjunction with the Act's redefinition of "electronic surveillance," is the cornerstone to the constitutional argument against the Protect America Act.

4. Oversight Proceduress

The Protect America Act provides a new framework for evaluating the intelligence gathering activities it authorizes. The Act requires certification that the collection activities meet five requirements.[112] However, unlike a warrant, certification need not "identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed."[113] Additionally, certification by the Director of National Intelligence and Attorney General may be oral instead of written if "time does not permit the preparation of a [written] certification, and the minimization procedures" established by those individuals.[114] The Protect America Act permits this truncated process, despite section 2(a)(5)'s requirement that the collection meet the minimization procedures in FISA sections 101H and 105B.[115]

Section 3 creates a "review process for the procedures under which the government determines that acquisitions of foreign intelligence information from persons reasonably believed to be located outside the United States do not constitute electronic surveillance."[116] This process requires that, within 120 days of the Act's passage, the Attorney General submit to FISC the procedures to determine whether activities conducted under the Act constitute electronic surveillance.[117] FISC then uses a "clearly erroneous" standard[118] to evaluate whether the "procedures are reasonably designed to ensure that acquisitions conducted pursuant to [the Act] do not constitute electronic surveillance."[119] Consequently, FISC does not provide impartial review of the acquisition procedures or even the acquisitions; FISC only reviews the criteria used to determine whether a procedure is "electronic surveillance." The clearly erroneous standard also gives tremendous deference to the intelligence community which develops the criteria. Unlike FISA section 104, where the government provides FISC with "substantive information about the electronic surveillance involved upon which the court can base its determinations[,] in the Protect America Act] the government submits certain procedures to the FISC for review, but does not

---

111 *Id.* § 2(a)(5).
112 *Id.* § 2(a)(1-5).
113 *Id.* § 2(b).
114 *Id.* § 2(a).
115 *Id.* § 2(a)(5).
116 BAZAN, *supra* note 10, at 13.
117 Protect America Act § 3(a).
118 *Id.* § 3(b).
119 *Id.*

provide the court with substantive information about the acquisitions themselves."[120]

5. The Sunset Clause

The Protect America Act's last provision is the six month sunset clause. Under the sunset provision, sections 2, 3, 4, and 5 expire 180 days from the Act's passage, February 1, 2008.[121] Though the sunset provision forced Congress to reconsider this legislation, the sunset provision neither protected Americans' civil liberties before the Act's expiration, nor protects their rights after it expires. Under Section 6(d), all authorizations of foreign intelligence information acquisitions under Section 2 "shall remain in effect until their expiration."[122] Thus, activities approved through the Act before, but set to expire after, February 1, 2008, remain authorized and functional. Therefore, even amendment or repeal would not necessarily curb the Act's effects. Contrary to its original purpose, the sunset clause did not provide any measure of constitutional protection.

6. Conclusion

The powers granted by the Protect America Act are inconsistent with FISA, despite the fact that the Act is codified within FISA. The Protect America Act provides fewer protections for Americans, greater discretion for the intelligence community, and fewer objective evaluations of government intelligence acquisition than does FISA. All of these distinctions render the Protect America Act constitutionally suspect. The issue is not whether information gathered under the Act is useful or whether the government finds incriminating information using these procedures. A constitutional violation occurs regardless of what the government does or does not find in exercising its Protect America Act powers. A Fourth Amendment violation occurs at the moment of unwarranted intrusion. Thus, the critical question is whether the Protect America Act violates Americans' constitutional rights by permitting unreasonable, warrantless surveillance of Americans.

PART V. THE PROTECT AMERICA ACT PERMITS FOURTH AMENDMENT VIOLATIONS

The Protect America Act implicates the Fourth Amendment because it permits domestic, warrantless surveillance. Supporters of the Act argue that Fourth Amendment electronic surveillance jurisprudence is irrelevant to the Act's application because the Act defined the activities it sanctions as *not* being

---

[120] BAZAN, *supra* note 10, at 13.

[121] Protect America Act § 6(c) ("Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 180 days after the date of the enactment of this Act.").

[122] *Id.* § 6(d).

electronic surveillance within the meaning of FISA, thus removing its activities from FISA's strictures. Such use of sly semantics should not circumnavigate the Fourth Amendment.

A. *Constitutional Concerns about "Concerning"*

With one word, the Protect America Act immediately implicates the Fourth Amendment. Section 2's meaning turns on Section 2(a)'s use of the word "concerning," which broadens the class of people at whom this surveillance activity can be directed. The relevant part of Section 2(a) reads:

> Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information *concerning* persons reasonably believed to be outside the United States[123]

Although the Act purports to close a loophole in foreign surveillance powers, this clause permits the United States' intelligence agencies to reach far beyond that purpose.[124] The statute's text permits the government to listen to conversations and collect emails between and among people who are in the United States, including United States citizens, without a warrant, provided that the communication is about a person "reasonably believed to be outside the country."[125] The section does not require the foreign target to be a party to the conversation being collected; the conversation need only be *about* that person and the sources may be American citizens inside the United States.[126] The Act accomplishes this by using the word "concerning" instead of "from."[127]

Neither the Protect America Act nor FISA define the term "concerning," therefore common usage is appropriate. The Oxford English Dictionary defines "concern" as "to distinguish, discern, perceive" or "to have relation or reference to; to refer to, relate to; to be about."[128] Using the common meaning of "concerning" to interpret the Protect America Act demonstrates that the information collected through the Act need only be *about* or *with reference to* a foreign target. For example, if Sally in Toledo were talking to George in Austin about their cousin, Jean, who was on vacation in Germany, the Protect America Act permits intelligence agencies to "collect" this conversation without a warrant. The only thing that the government needs to know before pro-

---

[123] *Id.* § 2(a) (emphasis added).

[124] *Id.* Preamble ("To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.").

[125] *Id.* § 2(a).

[126] *Id.*

[127] *Id.*

[128] Oxford English Dictionary, online version, *available at* http://dictionary.oed.com/cgi/entry/50046214?query_type=word&queryword=concerning&first=1&max_to_show=10&sort_type=alpha&search_id=0quV-j6cifb-6617&result_place=1.

ceeding with the collection is that the communication is about Jean, whom they reasonably believe to be outside of the United States. Contrary to administration and congressional statements,[129] the statute does not even require the government to suspect the subject of the conversation (Jean, in the example) of terrorist activities or of being a threat to national security.[130]

The critical point is that in Fourth Amendment jurisprudence the *person being searched* triggers the Fourth Amendment constitutional violation, *not the place or content* of the search.[131] Applied in this context, when the government monitors George and Sally's communications without a warrant or probable cause, their rights are violated. However, Jean's rights are not violated because she is merely the subject of George and Sally's communication. Although the government may seek information about Jean (the target of the surveillance), it is Sally's and George's constitutional rights that the government compromises. The end result is that the government violates the rights of the people whose communications it monitors, not the subject of the surveillance who is reasonably believed to be outside of the United States (and who could be a foreign national or a Untied States citizen). Thus, under the Protect America Act, in permitting surveillance of an American's communication *about* a foreign national, the government violates the American person's rights, not the foreign national's rights.

Another potential violation of Americans' rights arises because the Protect America Act does not provide language limiting permissible sources of information.[132] The Act includes language which limits communication collection specifically to communications about people outside of the United States,[133] but because the Act does not specify permissible or impermissible sources for that information,[134] the collection is virtually limitless; the source could be an American located within the United States. While the Act contains some limiting language,[135] it does not confine intelligence collection to information obtained *from* non-United States citizens[136] or *from* persons reasonably believed to be outside the United States;[137] the Act's sole limitation is to the subject of

---

[129] 153 CONG. REC. S10869 (daily ed. Aug. 3, 2007) (statement of Sen. Chambliss ("And we are not going to listen to any foreign caller unless we know they are a member of al-Quaida under current law."); Press Release, The White House, President George W. Bush, *supra* note 15 (statement of Scott McClellan, White House Press Secretary "The NSA's terrorist surveillance program is targeted at al Qaeda communications coming into or going out of the United States."). *See also* discussion *supra* Part III.

[130] Protect America Act § 2(a).

[131] United States v. Katz, 389 U.S. 347, 351, 353 (1967).

[132] *See generally,* Protect America Act.

[133] *Id.* § 2.

[134] *See generally,* Protect America Act.

[135] *Id.* § 2.

[136] *See generally,* Protect America Act.

[137] *Id.*

the collection.[138] By its silence, the Act permits warrantless, domestic spying, which is similar to the type of acquisition (intelligence gathering) regulated and prohibited by FISA's electronic surveillance definition.[139] The Protect America Act, however, lacks FISA protections strictly limiting such acquisitions.[140] Finally, the phrase "notwithstanding any other law," which begins Protect America Act section 2, asserts the Act's supremacy over other laws which may have otherwise limited it.[141]

B. *Redefining Electronic Surveillance*

By defining the activities authorized in the Protect America Act as something other than electronic surveillance, it appears that its drafters attempted to circumvent Fourth Amendment concerns. Had the drafters instead classified Protect America Act activities as electronic surveillance under FISA, such activities would be illegal if directed at United States citizens without probable cause and a warrant.[142]

As described in Part IV of this Note, section 2 of the Act states that "[n]othing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."[143] Because "shall" in statutory interpretation means "must," this section mandates that the Protect America Act's provisions not be interpreted as "electronic surveillance" as defined by FISA. But for this clause, the activities authorized by the Protect America Act could be included within FISA's "electronic surveillance" definition and consequently would come under FISA's protective requirements as discussed in Part IV.[144]

The activities set forth in the Protect America Act differ little from those in FISA. First, the Protect America Act does not specify the kind of collection procedures to which it applies. The Act does, however, refer to communications that are transmitted or stored on equipment, indicating electronic collection.[145] And, because the Act does not include language limiting the kind of collection procedure it permits, the Act does not preclude collection of electronic information, which is the kind of collection – electronic surveillance – for which FISA provides safeguards. Second, while FISA's definition of "electronic surveillance" specifically limits its own application to communications

---

[138] *Id.* § 2.

[139] FISA § 101(f).

[140] 50 U.S.C. §1801(f) (2006).

[141] Protect America Act of 2007 § 2(a).

[142] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972); United States v. Katz, 389 U.S. 347 (1967).

[143] Protect America Act § 2. *See supra* Part IV.

[144] *Supra* Part IV.

[145] *Id.* § 2(a)(3).

to or from an American citizen,[146] the Protect America Act does not preclude the government from directing its surveillance activities against an American in the United States. Third, the "electronic surveillance" definition includes a clause regarding an American citizen's expectation of privacy and a warrant requirement to collect private information.[147] These activities are governed by the FISA court protections.[148] Given the similarity of methodology and kind of collection – electronic devices and Americans in America– the Protect America Act intelligence collection should necessitate identical protections as FISA's "electronic surveillance" activities. In short, the activities outlined in the Protect America Act are virtually identical to those considered "electronic surveillance" under FISA, but are exempt from inclusion in the definition of "electronic surveillance" through suspiciously convenient semantics. Consequently, activities under the Act are also exempt from FISA's Fourth Amendment protections.

This language manipulation removes Protect America Act activities from the normal purview of FISC's and FISA's protections. The differences in language between FISA and the Protect America Act indicate that the Act's drafters intended that the surveillance activities and capabilities outlined in the Protect America Act be different from those in FISA. If that was not the intent, the drafters could have simply amended the definition of "electronic surveillance" to close FISA loopholes alleged by the Administration.[149] Instead, an isolated set of procedures govern these activities, and those procedures do not require a warrant or objective evaluation.

C. *The Fourth Amendment*

In addition to violating FISA, the activities permitted by the Protect America Act violate the Fourth Amendment because the Act permits unreasonable search and seizure.

1. The Protect America Act Permits Unreasonable Search and Seizure

Under the Protect America Act, U.S. intelligence agencies do not need a warrant, probable cause, or even a description of when or from whom they will collect information in order to conduct surveillance.[150] Each of these elements contrasts with the protections contained in FISA. First, the Act permits search and seizure without a warrant.[151] FISA, in contrast, "was an acknowledgement by Congress that the Fourth Amendment required prior judicial approval before the communications of Americans within the country could be monitored . . .

---

[146] *Id.* § 2(a)(3); FISA § 101F

[147] FISA § 101F.

[148] *Id.*

[149] Press Release, The White House, President George W. Bush, *supra* note 18.

[150] Protect America Act § 2.

[151] *See generally* Protect America Act.

for foreign intelligence purposes."[152] FISA was rooted in *Katz* and *Keith*.[153] In *Keith*, the Court held that "the President violated the Fourth Amendment by authorizing warrantless wiretaps in national security cases."[154] In that case, "no justice voted to uphold the government's claim that warrantless wiretaps in national security cases were reasonable under the Fourth Amendment."[155] Thus, even before FISA, the Supreme Court upheld the proposition that domestic wiretaps, even to promote national security, were unconstitutional without a warrant. FISA codified these sentiments by requiring third party approval of domestic surveillance by the FISA court.[156] The Protect America Act requires neither a warrant nor probable cause to conduct its surveillance activities.[157] The only standard the Act requires is "reasonable belief" that the person about whom the communication is collected is not in the United States, a lower standard than probable cause.[158] Probable cause is the historic and constitutionally sanctioned standard for government intrusions which implicate the Fourth Amendment, including those intrusions permitted by the Protect America Act.[159]

Second, the Protect America Act does not require intelligence agencies to describe the person, location, and/or information they seek, as required by the Fourth Amendment's particularity clause.[160] The particularity requirement for domestic surveillance is a cornerstone of Fourth Amendment jurisprudence. Under the Act, however, certification of these activities by the Director of National intelligence "is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence will be directed."[161]

Third, even if domestic wiretapping for foreign intelligence were constitutional under the special needs doctrine,[162] the primary purpose of Protect

---

[152] Maclin, *supra* note 77, at 1297-98.

[153] *Id*. at 1296-97; *United States v. U.S. Dist. Court* (*Keith*), 407 U.S. 297; *United States v. Katz*, 389 U.S. 347.

[154] Maclin, *supra* note 77, at 1263; *Keith,* 407 U.S. at 324.

[155] Maclin, *supra* note 77, at 1263; *Keith*, 407 U.S. at 323-24 (1972).

[156] 50 U.S.C. § 1801(f).

[157] Protect America Act of 2007 § 2.

[158] *Id.* For a Supreme Court discussion on the nature of probable cause and reasonable suspicion, see Ornelas v. United States, 517 U.S. 690, 695-96 (1996).

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

[160] *Id.*

[161] Protect America Act of 2007 Pub. L. No. 110-55, § 2(b), 121 Stat. 552, 553.

[162] The Special Needs Doctrine refers to the Court's assessment that there are times that call for an exception to the Fourth Amendment's Warrant Clause, when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." Skinner v. Ry. Labor Exec. Ass'n, 489 U.S. 602, 619 (1989) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).). *See also*, New Jersey v. T.L.O., 469 U.S. 325 (1985). In *Keith* the Court established that "[d]ifferent standards may be compatible

America Act surveillance does not need to be foreign intelligence collection to be permissible under the statute.[163] The Act states only that "a *significant* purpose of the acquisition [must be] to obtain foreign intelligence information."[164] Thus, although the Act's asserted purpose was to further national security goals, that does need to be the primary or only impetus for collecting intelligence under the Act.[165] Conducting warrantless, domestic, surveillance activities for purposes other than discovering terrorist activities is therefore also permissible under the Act.[166]

Fourth, the Protect America Act leaves open the question of whether information gathered through its procedures could be used in other legal contexts. If potentially incriminating evidence were discovered during a Protect America Act collection, that information could potentially be used in an unrelated investigation. For example, if, while authorities listened to Sally and George's conversation, Sally mentioned she just robbed a bank or accepted delivery of 2 kilos of cocaine, it is possible that Sally's statement could be used against her in an ordinary civil or criminal proceeding. The Act's alleged purpose is to provide additional procedures to acquire foreign intelligence,[167] but its permissions are broader; it could potentially lead to the collection and use of information with no bearing on terrorism or national security. This question has yet to be answered; however the assumption remains that laws are constitutional until a court rules otherwise. Therefore, unless a court rules otherwise, it appears that any information acquired under the Protect America Act could be used in other legal contexts.

Part VI. Implications and Conclusion

Though the Protect America Act has been amended,[168] the Act, as originally passed, remains relevant. Between August 5, 2007, and February 1, 2008, the Act permitted United States intelligence communities to engage in warrantless, domestic surveillance authorized by Congress and the President.[169] Information on how many constitutional violations, if any, occurred under the Act is unavailable. Those who suspect their rights were violated have no judicial

---

with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection." United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 322-23 (1972).

[163] Protect America Act § 2(a)(4).

[164] Protect America Act § 2(a)(4) (emphasis added).

[165] *Id.*

[166] *Id*.

[167] *See* discussion *supra* Part III.

[168] FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008).

[169] *See* discussion *supra* Part V.

remedy after *American Civil Liberties Union v. National Security Agency*.[170] There, the Sixth Circuit held that the complainants did not have standing to bring a claim against the NSA's wiretapping program because they could not prove that they had been wiretapped by the NSA.[171] Ironically, these people could not prove harm because the list of those affected by surveillance is classified and production of such evidence cannot be compelled through subpoena or other discovery processes.[172] While the scope of violations is unclear, it *is* clear that the Act permits unconstitutional surveillance activities.[173] Even if the government never uses the information it gains through these procedures, violations occur at the very exercise of this power.

The Protect America Act of 2007 expired on February 1, 2008. Congress and the President extended the Act for six months, and on July 9, 2008 President Bush signed into law new amendments to FISA.[174] The permanent FISA amendments include different and potentially less constitutionally suspect language than does the Protect America Act.[175] Although the new language appears to be less constitutionally suspect, these new amendments provide immunity to companies which aid the government in collections procedures.[176] Once again, United States citizens are left without a remedy for constitutional violations. Additionally, these amendments do nothing to remedy Fourth Amendment violations which potentially occurred between August 5, 2007, and February 1, 2008. Nor does amending the Act reveal how many Americans' conversations and/or emails were warrantlessly searched and seized by the government. Thus, this Act's history and implications remain important.

The Bush Administration continues to claim that the purpose of the Protect America Act and subsequent, related amendments is to gather foreign intelligence (particularly from al Qaeda), which protects the Nation from terrorist attacks.[177] It claims that the Protect America Act does not permit domestic

---

[170] Am. Civ. Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2007); Am. Civ. Liberties Union v. Nat'l Sec. Agency, No. 07-468, 2008 WL 423556, *cert. denied,* (128 S. Ct. 1334 (2008)).

[171] *Id.*

[172] *In Re* Motion for Release, No. Misc 07-01 (For. Intell. Surveillance Ct. 2007) *available at* http://www.aclu.org/pdfs/safefree/fisc_order_2007_1211.pdf.

[173] *See* discussion *supra* PartV.

[174] FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008). For specific transition procedures from operation under the Protect America Act to the permanent amendments under the FISA Amendments Act of 2008 *see* 50 U.S.C.A. § 1881a. For Executive reaction, *see* Press Release, The White House, President George W. Bush, President Bush Pleased by Passage of FISA Reform Legislation (July 9, 2008) (the President described that bill as "help[ing] our intelligence professionals learn who the terrorists are talking to, what they're saying, and what they're planning.")

[175] 50 U.S.C.A. § 1881a (2008).

[176] 50 U.S.C.A. § 1885 (2008).

[177] Press Release, The White House, *supra* note 172; Press Release, The White House,

warrantless surveillance.[178] First, then, let this be a lesson in careful legislative drafting. Second, if permitting warrantless domestic surveillance was not the Act's intention, then amendment process should signal the Act's "true" legislative intent and prevent future Fourth Amendment violations (the amendment process could not correct past constitutional violations).

The Protect America Act permits unconstitutional, warrantless, domestic surveillance. Although the Act's asserted purpose is to collect foreign intelligence, because of FISA's definition of foreign intelligence, and the Act's careful language choice,[179] the asserted purpose does not limit operation of the Protect America Act's activities to international sources and non-US citizens. This authority, given to the American intelligence community by both Congress and the President, is a significant departure from established American national security law and Fourth Amendment jurisprudence; it impinges upon the fundamental constitutional right of Americans to be free from unreasonable search and seizure.

President George W. Bush, Myth/Fact: Key Myths About FISA Amendments in the Protect America Act (Sept. 18, 2007), http://www.whitehouse.gov/news/releases/2007/09/20070918-1.html.

[178] *Id. See e.g.,* Press Release, The White House, George W. Bush, Statement by the Press Secretary on FISA (Feb. 25, 2008); Press Release, The White House, George W. Bush, Fact Sheet: The House Must Act Quickly to Pass Bipartisan Senate FISA Modernization Bill (Feb. 13, 2008).

[179] *Supra* Part V.A.