

In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*

Matthew A. Anzaldi** & Jonathan W. Gannon***

I. Introduction

Mere hours before adjourning for its August 2007 recess,¹ Congress amended the Foreign Intelligence Surveillance Act (FISA)² and enacted the Protect America Act of 2007.³ Congress took up the measure based upon concerns raised by the Director of National Intelligence (DNI) that FISA required immediate modernization in the face of a “heightened terrorist threat environment” to address the needs of the U.S. Intelligence Community and to remove FISA’s “requirement of a court order to collect foreign intelligence about foreign targets located overseas.”⁴ Among other things, the Protect America Act authorized the DNI and the Attorney General to conduct foreign intelligence surveillance concerning persons reasonably believed to be outside the United States without obtaining a warrant or other court order.⁵

Debate over the Protect America Act focused on the extent to which it safeguarded the privacy interests of U.S. persons.⁶ Supporters of the

* The views expressed in this Article are solely those of the authors and do not necessarily represent the views of any other person or entity, including the Department of Justice. This Article has been submitted for prepublication review pursuant to 28 C.F.R. § 17.18 (2009) and cleared for publication. The authors, among others, received the National Security Division Assistant Attorney General’s Award for Special Initiative for their work on the matter discussed in this Article. The authors would like to thank their colleagues at the Department of Justice and the other Symposium participants for their review and comments on this Article.

** Attorney Advisor, Office of Intelligence, National Security Division, U.S. Department of Justice. A.B., 1993, Duke University; J.D., 1996, Vanderbilt University Law School.

***Deputy Unit Chief, Office of Intelligence, National Security Division, U.S. Department of Justice. B.A., 1995, College of the Holy Cross; J.D., 2000, Vanderbilt University Law School.

1. See Eric Lichtblau et al., *Reported Drop in Surveillance Spurred a Law*, N.Y. TIMES, Aug. 11, 2007, at A1 (describing the “fever pitch” of negotiations going into the August recess).

2. Foreign Intelligence Surveillance Act of 1978, Pub L. No. 95-511, 92 Stat. 1783, (codified as amended in scattered titles of the U.S.C.).

3. Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c). For a discussion of the legislative history of the Protect America Act, see generally ELIZABETH B. BAZAN, CONG. RESEARCH SERV., P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2008), available at <http://www.fas.org/sgp/crs/intel/RL34143.pdf>.

4. S. REP. NO. 110-209, at 6 (2007).

5. Protect America Act § 2.

6. See FISA § 101 (codified at 50 U.S.C. § 1801(i) (2006)) (defining “United States person[s]” primarily as citizens and permanent resident aliens of the United States); S. REP. NO. 110-209, at 5

legislation argued that the Protect America Act would restore FISA's original balance between protections for persons communicating within the United States and the Executive Branch's traditional authority to conduct certain warrantless surveillance.⁷ Critics declared that the legislation would authorize unconstitutional, warrantless surveillance of the communications of U.S. persons, would transfer power from the courts to the Executive Branch, and would place excessive authority in the hands of the Attorney General and the DNI.⁸ About one thing, at least, supporters and critics agreed: the adjournment deadline did not afford the time necessary to analyze the legislation sufficiently.⁹ The legislation, therefore, included a six-month sunset provision.¹⁰ As one member noted, "To state the obvious: This is a very troublesome way to legislate."¹¹

During the following months, while Congress considered changes to the Protect America Act, a communications service provider challenged on Fourth Amendment grounds the constitutionality of the legislation in classified proceedings before the Foreign Intelligence Surveillance Court (FISC or FISA Court) and later, on appeal, before the Foreign Intelligence Surveillance Court of Review (Court of Review).¹² The Court of Review's

(describing how Director of National Intelligence J. Michael McConnell's proposal to modernize the Foreign Intelligence Surveillance Act intended to preserve "the privacy interests of persons in the United States").

7. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 30 (2007) [hereinafter *Modernization of FISA*] (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice ("We can and should amend FISA to restore its original focus on foreign intelligence activities that substantially implicate the privacy interests of individuals in the United States.")).

8. *See, e.g.*, American Civil Liberties Union, *ACLU Fact Sheet on the "Police America Act,"* (Aug. 7, 2007), <http://www.aclu.org/safefree/nsaspying/31203res20070807.html> (arguing that the Protect America Act "allows for massive, untargeted collection of international communications without court order or meaningful oversight by either Congress or the courts" and that the Act provides "no protections for the U.S. end of the phone call or email, leaving decisions about the collection, mining and use of Americans' private communications up to this administration").

9. For example, Senator Russ Feingold, who voted against the Protect America Act, called it a "cynical, cynical abuse of the process" when, in his view, the Bush Administration delayed negotiations on the bill and then rushed it through just before the August adjournment. David Sarasohn, *Rewriting the Surveillance Rules*, OREGONIAN, Oct. 10, 2007, at B8; *see also* Editorial, *Stampeding Congress, Again*, N.Y. TIMES, Aug. 3, 2007, at A18 (criticizing the Bush Administration for rushing the Act's passage just prior to the August recess). For statements by bill supporters alluding to the lack of time allowed for deliberation, *see infra* notes 11 and 93. *But see* 153 CONG. REC. S10,860 (daily ed. Aug. 3, 2007) (statement of Sen. Hatch) ("Is the excuse [for not passing the Act] that we might not have enough time before recess? Of course we have time. We'll make time.").

10. Protect America Act of 2007, Pub. L. No. 110-55, § 6, 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803 n.3).

11. 153 CONG. REC. S10,869 (daily ed. Aug. 3, 2007) (statement of Sen. Specter). Senator Specter voted for the Protect America Act. *Id.* at S10,870; *see also* S. REP. NO. 110-209, at 6 ("The [Protect America Act] sparked serious concerns about its reach and scope [The Senate Select Committee on Intelligence] immediately began to review the Act's implementation.").

12. *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1007-08 (FISA Ct. Rev. 2008) [hereinafter *In re Directives*].

decision on this challenge in *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (In re Directives)*¹³ upheld the Protect America Act as implemented by the Executive Branch.¹⁴ In so doing, the Court of Review expressly recognized a foreign intelligence exception to the Warrant Clause of the Fourth Amendment “when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.”¹⁵ The Court of Review also held that the warrantless surveillance, as implemented, satisfied the Fourth Amendment’s reasonableness requirement, even when the government acquires communications of U.S. persons who are not the targets of the surveillance.¹⁶ These holdings answer some of the principal criticisms of the Protect America Act. They also are a contemporary reminder that certain surveillances and searches conducted by the Executive Branch without prior judicial review do not violate the Fourth Amendment, at least when such activity is expressly authorized by Congress and subject to appropriate privacy protections.

II. Executive Branch Authority to Collect Foreign Intelligence Without a Court Order Before Enactment of the Protect America Act

For much of the nation’s history, the Executive Branch exercised largely unchecked discretion in gathering foreign intelligence. That changed in 1978 with the enactment of FISA, but even then certain methods of foreign intelligence collection, including those later implicated in the Protect America Act, continued to involve only the Executive Branch.

A. Foreign Intelligence Collection Prior to 1978 and Resulting Abuses

Before FISA, the Executive Branch conducted surveillance for foreign intelligence purposes without significant oversight by Congress or the

13. *Id.* at 1004.

14. *Id.* at 1016. The decision discussed herein is only the second opinion released by the Court of Review, which is comprised of three judges from United States district courts or courts of appeals who have been publicly designated by the Chief Justice. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103, 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1803(b) (2006)). Although the court entertained amicus briefs from the American Civil Liberties Union and the National Association of Criminal Defense Lawyers in *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002), that matter was an *ex parte* proceeding. *Id.* at 721 n.6.

15. *In re Directives*, 551 F.3d at 1012. The Fourth Amendment provides,

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 particularly describing the places to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

16. *In re Directives*, 551 F.3d at 1015.

courts.¹⁷ Beginning with George Washington, a “master of military espionage,”¹⁸ presidents had conducted surveillance to collect foreign intelligence using an evolving array of techniques to account for changing technologies.¹⁹ Electronic surveillance—the interception of communications as they travel on a wire—began shortly after the development of electronic communication.²⁰ Electronic surveillance of wartime communications was conducted as far back as the Civil War, and President Wilson ordered the censorship of messages sent via wire during World War I.²¹ Before the country’s entry into World War II, President Roosevelt also authorized the warrantless surveillance of “persons suspected of subversive activities against the Government of the United States, including suspected spies.”²²

At the time, electronic surveillance implemented solely by the Executive Branch did not raise Fourth Amendment concerns because, as held by the Supreme Court in *Olmstead v. United States*,²³ wiretapping was not considered a search within the meaning of the Fourth Amendment.²⁴ The Supreme Court changed course in 1967, holding in *Katz v. United States*²⁵ that electronic surveillance implicated the Fourth Amendment.²⁶ Still, even after *Katz* recognized Fourth Amendment protections for certain electronic

17. See DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 3-2 (2007) (describing how, before FISA’s 1978 enactment, electronic surveillance was subject to little or no congressional or legislative oversight). The President derives the power to gather intelligence from his Article II authorities. Specifically, the President is Commander in Chief of the Armed Forces and controls the foreign affairs of the United States. U.S. CONST. art. II, § 2. The Supreme Court has recognized that the President “is the sole organ of the nation in its external relations, and its sole representative with foreign nations.” *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (citation omitted). Extending from these responsibilities is the President’s constitutional responsibility to protect the nation from foreign threats. U.S. DEP’T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 7 (2006) [hereinafter DOJ WHITEPAPER] (“[T]he Founders . . . intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation’s foreign affairs.”).

18. RHODRI JEFFREYS-JONES, CLOAK AND DOLLAR: A HISTORY OF AMERICAN SECRET INTELLIGENCE 11 (2d ed. 2003); see also ALLEN W. DULLES, THE CRAFT OF INTELLIGENCE 49 (1st ed. 1965) (discussing Washington’s observation in 1777 that “[t]he necessity of procuring good intelligence is apparent and need not be further urged”).

19. See, e.g., DOJ WHITEPAPER, *supra* note 17, at 14–16 (2006) (describing certain aspects of the history of wartime surveillance).

20. KRIS & WILSON, *supra* note 17, at 3-3 (citation omitted).

21. DOJ WHITEPAPER, *supra* note 17, at 16 (citing G.J.A. O’TOOLE, THE ENCYCLOPEDIA OF AMERICAN INTELLIGENCE AND ESPIONAGE 498 (1988) and Exec. Order No. 2604 (Apr. 28, 1917)).

22. KRIS & WILSON, *supra* note 17, at 3-6.

23. 277 U.S. 438 (1928).

24. *Id.* at 465 (“The language of the [Fourth] Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant’s house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.”).

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

26. *Id.* at 353–54.

communications, the Executive Branch continued to operate without judicial or legislative checks.²⁷

Congress subsequently sought to regulate government wiretapping, but only in the context of criminal investigations.²⁸ In response to the Supreme Court's decisions in *Katz* and *Berger v. New York*,²⁹ and in an era of "increasing use and sophistication of electronic surveillance,"³⁰ Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).³¹ While Title III barred electronic surveillance except under the circumstances set forth in the statute, Congress expressly avoided the regulation of foreign intelligence surveillance.³²

The Supreme Court also generally remained silent on the question of Fourth Amendment protections and foreign intelligence gathering. In *Katz*, the Court stated that its holding did not apply to a situation involving national security: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."³³ Several years later in *United States v. United States District Court (Keith)*,³⁴ the Government argued that § 2511(3) of Title III authorized warrantless surveillance of a domestic radical group.³⁵ The Court steered clear of the question of

27. DOJ WHITEPAPER, *supra* note 17, at 8, 17.

28. Congress enacted a criminal penalty prohibiting wiretapping of telephones during World War I and made it a crime for any person without the consent of the sender to "intercept and divulge or publish the contents of wire and radio communications" in § 605 of the Federal Communications Act of 1934. 47 U.S.C. § 605 (1934); KRIS & WILSON, *supra* note 17, at 3-3 to 3-5.

29. 388 U.S. 41, 44 (1967) (holding a New York statute regulating electronic eavesdropping to be unconstitutional).

30. KRIS & WILSON, *supra* note 17, at 3-13.

31. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2006)).

32. See JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE 9-5 (2007) ("Because a court order authorizing FISA surveillance differs in significant ways from a conventional search warrant, however, the adoption of FISA did not itself resolve other questions about when and under what conditions the Constitution permits foreign intelligence surveillance."). As enacted in 1968, 18 U.S.C. § 2511(3) provided, among other things, that nothing in Title III or § 605 of the Federal Communications Act of 1934 "shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, [or] to obtain foreign intelligence information deemed essential to the security of the United States." 18 U.S.C. § 2511(3) (1970). This provision was removed in 1978. CARR & BELLIA, *supra*, at 9-4; see also *id.* at 9-2 ("Section 2511(3) was intended as a codification of the legislative 'hands off' attitude which had prevailed under Title III's predecessor." (citations omitted)).

33. *Katz v. United States*, 389 U.S. 347, 358 n.23 (1967). Seizing upon the majority's caveat for national security, Justice White observed that "[w]e should not require the warrant procedure . . . if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Id.* at 364 (White, J., concurring).

34. 407 U.S. 297 (1972)

35. *Id.* at 303.

warrantless surveillance for foreign intelligence gathering.³⁶ In concluding that the warrant requirement applied to investigations of domestic security threats, the *Keith* Court expressly reserved the question of whether the Warrant Clause applied to foreign intelligence surveillance and discussed several sources supporting the “view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved.”³⁷

This era of Executive Branch flexibility and warrantless foreign intelligence wiretapping came to an end with the well-documented abuses of the civil rights of U.S. persons uncovered by Congress through the Church Committee.³⁸ While the Intelligence Community often began investigations with legitimate national security concerns, the investigations “descended a slippery slope, beginning with efforts to counter foreign threats to national security and evolving to gather information about peaceful domestic groups lobbying for political change, such as equal rights for racial minorities and women.”³⁹ The abuses “included routine opening and reading of vast amounts of first-class mail and telegrams.”⁴⁰ One program run by the National Security Agency (NSA) was called “Operation Shamrock.”⁴¹ Originally intended to “obtain the enciphered telegrams of certain foreign targets,” Operation Shamrock expanded significantly over time to become at that time “the largest government interception program affecting Americans.”⁴² As a result of the program, from approximately 1945 to 1975 the NSA received copies of millions of international telegrams sent to, from,

36. *See id.* at 321–22 (“[T]his case involves only the domestic aspects of national security. We . . . express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”). Perhaps foreshadowing the creation of the FISC, the *Keith* Court rejected the Government’s argument that “internal security matters are too subtle and complex for judicial evaluation There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases.” *Id.* at 320. The Supreme Court further suggested that Congress should consider protective standards for domestic security cases different than those for criminal cases (Title III), including applications to a “specially designated court.” *Id.* at 323.

37. *Id.* at 322 n.20. As will be described below, while the Supreme Court has remained silent on the specific issue, prior to the decision discussed herein courts of appeals in the pre- and post-FISA context have held that the President has authority to conduct warrantless surveillance in cases involving foreign intelligence collection. *See infra* text accompanying notes 135–39.

38. In January 1975, the Senate created the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church, to investigate the activities of intelligence agencies. L. Britt Snider, *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years*, at 1 n.3, <http://www.law.duke.edu/lens/downloads/snider.pdf>. In February 1975, the House of Representatives established the Select Committee on Intelligence, chaired by Representative Otis Pike, for the same purpose. *Id.*

39. KRIS & WILSON, *supra* note 17, at 2–3.

40. *Id.*

41. S. REP. NO. 94-755, at 740 (1976).

42. *Id.*

or transiting the United States; in later years, the NSA reviewed approximately 150,000 telegrams per month.⁴³

B. 1978 to 2007: Executive Branch Adjustment to FISA

With the enactment of FISA in 1978, Congress entered the field of electronic surveillance for foreign intelligence purposes.⁴⁴ Congress enacted FISA to establish “a statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.”⁴⁵ When FISA applies, it generally requires the government to seek an order from the FISC approving the use of “electronic surveillance” to obtain “foreign intelligence information,” which is defined as, *inter alia*, information that relates to the ability of the United States to protect against espionage, international terrorism, and other acts committed by foreign powers or their agents, as well as other information pertaining to the national defense and foreign affairs of the United States.⁴⁶ Among other things, the FISC must find that the government has established probable cause to believe that (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power, and (2) the target is using or is about to use the facility at which surveillance will be directed.⁴⁷ The FISC must also find that the minimization procedures proposed by the government are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting U.S. persons consistent with

43. *Id.*

44. Oversight of the intelligence agencies previously had fallen largely to subcommittees of the Senate and House Armed Services Committees. See Snider, *supra* note 38, at 2 (“Such oversight, as there was, was carried out in secret and in a relative vacuum.”). Congress later established committees specifically designed to conduct oversight of intelligence activities: the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The Senate created SSCI in 1976 as the successor to the Church Committee, and the House created HPSCI in 1977 as the successor to the Pike Committee. See L. BRITT SNIDER, *THE AGENCY AND THE HILL: CIA’S RELATIONSHIP WITH CONGRESS, 1946–2004*, at 51, 53 (2008) (describing the inception of those committees). The Protect America Act contained certain reporting requirements to Congress, such as section four, beyond those in FISA generally. See, e.g., 50 U.S.C. § 1808 (2006) (requiring the Attorney General to report semi-annually to the SSCI and HPSCI on the government’s electronic surveillance activities).

45. H.R. REP. NO. 95-1283, at 22 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3923–24.

46. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783, 1784 (codified at 50 U.S.C. § 1801(e) (2006)). The legislative history indicates that Congress specifically excluded from FISA certain Executive Branch authorities, including “international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance . . . conducted outside the United States.” S. REP. NO. 95-604, at 64 (1978); see also H.R. REP. NO. 95-1283, at 27 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3928–29 (“The Committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillance.”).

47. FISA § 101. As noted below, the Protect America Act specifically provided that the government need not provide an individual probable cause statement for each target or facility. See *infra* note 102 and accompanying text.

the need of the United States to obtain, produce, and disseminate foreign intelligence information.”⁴⁸

FISA’s definition of electronic surveillance determines the reach of the statute, and by adopting the definition, Congress left untouched much of the foreign intelligence collection that was directed overseas and conducted solely on the basis of Executive Branch authority.⁴⁹ Only electronic surveillance, as defined in four parts, requires judicial approval.⁵⁰ The first definition of electronic surveillance is the acquisition of a “wire or radio communication” to or from “a particular, known United States person who is in the United States”⁵¹ This definition does not regulate the surveillance of targets located outside the United States.⁵² The second definition of electronic surveillance is the acquisition of a “wire communication,” defined as a communication carried on a wire by common carriers, to or from someone in the United States.⁵³ This definition did not regulate the surveillance of the most common manner of international communications.⁵⁴ At the time of

48. FISA § 101. Section 1801(h) defines “minimization procedures” in four parts, the most pertinent of which is quoted above. As discussed below, the Protect America Act incorporated FISA’s general definition of minimization procedures. *See infra* note 101 and accompanying text.

49. As noted at the SSCI hearing in May 2007, FISA “does not apply where all parties to a communication are located abroad. Purely foreign communications are simply beyond FISA’s ambit.” *Modernization of FISA, supra* note 7, at 130 (statement of David S. Kris).

50. FISA itself recognizes several instances when the Executive Branch could conduct warrantless “electronic surveillance.” First, 50 U.S.C. § 1802 permits surveillance without judicial approval for periods of up to one year based solely upon a certification of the Attorney General when either the surveillance is solely directed at the acquisition of (1) the “contents of communications transmitted by means of communications used exclusively between or among foreign powers,” or (2) “technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power.” FISA § 102. Moreover, the government may conduct electronic surveillance upon oral authorization of the Attorney General in emergency situations. *Id.* § 105. The period of surveillance for an emergency authorization without a warrant has been extended from 24 hours (1978) to 72 hours (2001) to seven days in the FISA Amendments Act of 2008. Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2439–40 (to be codified at 50 U.S.C. § 1881(a)). An application must be submitted to the FISC after such authorization. FISA § 105. Third, the Executive Branch may conduct electronic surveillance without a warrant for fifteen calendar days after a congressional declaration of war. *Id.* § 111. Finally, FISA permits certain testing of electronic equipment and training of intelligence personnel without judicial approval. *Id.* § 105.

51. FISA § 101. During the Protect America Act debate, Administration officials sought to reassure Congress that FISA’s reach had not changed with respect to this definition of electronic surveillance. *See, e.g., Modernization of FISA, supra* note 7, at 27 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice) (“[I]f the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence purposes, it is within FISA’s scope, period.”); *id.* at 12 (statement of J. Michael McConnell, Director of National Intelligence) (“Another thing that this proposed legislation does *not* do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States persons.”).

52. FISA § 101.

53. *Id.*

54. *See id.* (excluding satellite transmissions from this definition of electronic surveillance).

FISA's enactment, most international communications were carried primarily by satellite (i.e., radio), not wire.⁵⁵

The third definition of electronic surveillance applies to the acquisition of a "radio communication" only when "both the sender and all intended recipients are located within the United States."⁵⁶ Here, too, the definition does not regulate the surveillance of targets outside the United States.⁵⁷ Finally, the fourth definition of electronic surveillance relates to the "installation of an electronic, mechanical, or other surveillance device in the United States" but excludes information acquired from a "wire or radio communication."⁵⁸ As with the second definition, this definition of electronic surveillance excluded, as a matter of communication technology, the most common form of international communications: satellite.⁵⁹

These definitions made FISA's scope, particularly with respect to the international communications of targets outside the United States, to some extent dependent on the communication technology in use at a given time.⁶⁰

55. *Modernization of FISA*, *supra* note 7, at 28–29 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice); cf. David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* 7–13 (Brookings Inst., Geo. Univ. Law Center, & Hoover Inst., Paper No. 1, 2007), available at http://www.brookings.edu/~media/Files/rc/papers/2007/1115_nationalsecurity_kris/1115_nationalsecurity_kris.pdf (estimating that between one-half and two-thirds of overseas calls were carried on satellites at the time of FISA's enactment).

56. FISA § 101.

57. *Id.*

58. *Id.*; see also H.R. REP. NO. 95-1283, at 52 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3953–54 (noting that § 1801(f)(4) was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States").

59. FISA § 101.

60. The Executive Branch developed procedures for the conduct of foreign intelligence, including foreign intelligence gathering outside of FISA. The enactment of FISA in 1978 created the framework within which the Executive Branch conducted electronic surveillance within the United States for foreign intelligence purposes, and applications to the FISC increased during subsequent years. Executive Order 12,333, which has been amended as recently as 2008, outlines the responsibilities and limitations of the agencies of the Intelligence Community. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Feb. 29, 2008). For example, the Attorney General maintained certain authority to authorize warrantless surveillance through section 2.5 of Executive Order 12,333, which among other things regulates the use of any technique against a U.S. person outside the United States. See Exec. Order No. 12,333, 3 C.F.R. 200 (1982), as amended by Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), reprinted as amended in 50 U.S.C. § 401 (2006) (empowering the Attorney General to use techniques "for which a warrant would be required" against U.S. persons abroad who are thought to be an "agent of a foreign power"). Section 2.5 provides in relevant part:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that . . . the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

If such international communications were carried by radio and satellite, FISA did not require a court order for government surveillance; if they were carried by wire, FISA might require an order.

III. The Protect America Act

A. *Debating the Protect America Act*

Before passage of the Protect America Act, changes in communications technology had, according to Administration officials, increased FISA's scope at the expense of Executive Branch authority.⁶¹ International communications, once mostly transmitted by satellite, were now transmitted by wire.⁶² New methods of communicating, including e-mail, became commonplace.⁶³ In summary, by operation of FISA's definition of electronic surveillance, FISA grew to encompass the surveillance of foreign intelligence targets outside the United States where, in the past, that surveillance might have been conducted without the requirement of a FISC order.⁶⁴

Changes in communications technology alone did not lead to serious proposals to restore FISA's original scope. Rather, plans to update FISA followed a new threat to national security and the increased (and, some claimed, consuming) number of applications for FISC authorization to target persons outside the United States.⁶⁵ These plans got a push after "any elec-

Id. As noted below, FISA now requires that such surveillance receive FISC approval. *See infra* text accompanying notes 232–33. Agencies have implemented the Executive Order through specific regulations. For example, Department of Defense (DOD) regulations require a statement of facts demonstrating probable cause and necessity and a statement of the period during which the surveillance was thought to be required, not to exceed 90 days. Department of Defense, DOD 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, 25–27 (Dec. 1982). This durational limit is the same as the limit authorized for an electronic surveillance order of a U.S. person pursuant to 50 U.S.C. § 1805. FISA § 105(d)(1). As discussed below, these procedures played an important role in the Court of Review's holding that the government acted reasonably under the Fourth Amendment in implementing the Protect America Act. *See In re Directives*, 551 F.3d 1004, 1013–14 (FISA Ct. Rev. 2008) (asserting that the procedures "serve to allay the probable cause concern"); *infra* subpart IV(B).

61. *Modernization of FISA*, *supra* note 7, at 29–30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice). NSA had earlier raised issues concerning tension between FISA's scope and NSA's collections given technological advances. *See* Memorandum from Mary C. Lawton, Counsel for Intelligence Policy, U.S. Dep't of Justice, to Dan Levin, Office of the Deputy Attorney Gen., U.S. Dep't of Justice 1 (Nov. 1, 1990), available at http://gulcfac.typepad.com/georgetown_university_law/files/Lawton.1990.FISA.Memo.clean.pdf (noting that the Department of Justice had been working with NSA for the previous three years to develop amendments to FISA "to meet a need created by technological advances").

62. *Modernization of FISA*, *supra* note 7, at 30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice).

63. *Id.* at 6 (statement of J. Michael McConnell, Director of National Intelligence).

64. *Id.* at 6–7 (statement of J. Michael McConnell, Director of National Intelligence).

65. As noted by Administration officials during the Protect America Act debate, the preeminent threat to the United States at the time of FISA's enactment was espionage by the Soviet Union and its agents and terrorism threats stemming from groups such as Black September, the Baader-Meinhof Group, and the Japanese Red Army, not international terrorism from groups such as al

tronic surveillance that was occurring as a part of the Terrorist Surveillance Program” (TSP) moved from Executive Branch authorization to FISC authorization in January 2007.⁶⁶

In the aftermath of the September 11, 2001 terrorist attacks, the use of FISA expanded dramatically.⁶⁷ The Director of the NSA stated in 2007 that FISA was “the key to the war on terrorism.”⁶⁸ Shortly after September 11, 2001, however, President George W. Bush authorized the NSA to operate outside of FISA “to intercept communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations.”⁶⁹ This authorization and the government’s subsequent effort to bring these activities before the FISC contributed in part to the legislative debate surrounding the Protect America Act. Specifically, on January 10, 2007, the FISC issued orders authorizing the government “to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.”⁷⁰ Later in 2007, in response to a request to renew the January 2007 FISA orders, a different FISC judge issued a subsequent ruling in May 2007 that the DNI and others apparently could not accept.⁷¹ The Executive Branch turned to Congress to act.⁷²

Qaeda. *Modernization of FISA*, *supra* note 7, at 28 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice).

66. See U.S. DEP’T OF JUSTICE, NATIONAL SECURITY DIVISION PROGRESS REPORT 2 (2008) [hereinafter NSD PROGRESS REPORT] (detailing the National Security Division’s role in legislation to update FISA); Letter from Alberto Gonzales, Att’y Gen., to Patrick Leahy, Chairman, Senate Comm. on the Judiciary and Arlen Specter, Ranking Minority Member, Senate Comm. on the Judiciary 1 (Jan. 17, 2007), available at www.fas.org/irp/agency/doj/fisa/ag011707.pdf [hereinafter January 2007 Attorney General Letter]; see also James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing an NSA collection).

67. As required by FISA, the Department of Justice reports semi-annually to Congress the number of applications filed with the FISC. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 108, 93 Stat. 1783, 1783 (codified at 50 U.S.C. § 1808(a)) (requiring the Attorney General to report on FISA surveillance to the SSCI and HPSCI). The number of FISA applications increased from 932 in 2001 to 2371 in 2007. See KRIS & WILSON, *supra* note 17, app. G, at G-3 to G-35 (collecting annual reports for calendar years 1980 to 2006); Report from Principal Dep. Att’y Gen. Brian A. Benczkowski to Sen. Harry Reid (Apr. 30, 2008), available at http://www.justice.gov/nsd/foia/reading_room/2007fisa-ltr.pdf (containing 2007 annual report to Congress). The number of applications dropped to 2082 in 2008, the year after the Protect America Act’s enactment. Report from Ass’t Att’y Gen. Ronald Weich to Sen. Harry Reid (May 14, 2009), available at http://www.justice.gov/nsd/foia/reading_room/2008fisa-ltr.pdf.

68. *Modernization of FISA*, *supra* note 7, at 48 (testimony by Keith B. Alexander, Director, National Security Agency).

69. DOJ WHITEPAPER, *supra* note 17, at 1. A discussion of the NSA’s surveillance activities other than their effect on the legislative debate is outside the scope of this Article.

70. January 2007 Attorney General Letter, *supra* note 66, at 1.

71. S. REP. NO. 110-209, at 5 (2007). The report describes the situation as follows:

At the end of May 2007, however, attention was drawn to a ruling of the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information to the Court.

In response to a request from the Senate Select Committee on Intelligence (SSCI), on April 12, 2007, the DNI submitted a proposal to Congress to modernize FISA.⁷³ While recognizing that FISA “provides the legal framework through which the Intelligence Community lawfully collects information about those who pose national security threats to our country,” the Department of Justice and Office of the DNI stated that the proposed legislation’s “core objective 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 interests of persons located in the United States.”⁷⁴

On May 1, 2007, SSCI held the only significant hearing on FISA modernization before the Protect America Act’s enactment.⁷⁵ The hearing foreshadowed the arguments for and against the initiative that would arise during the debate a few months later.⁷⁶ The DNI, the Director of the NSA

Id.

72. Similar to the events leading to the original passage of FISA, the Protect America Act debate also occurred against the backdrop of recently revealed abuses in the Intelligence Community. In March 2007, the Department of Justice’s Inspector General released a highly critical report of the FBI’s use of national security letters from 2003 to 2005. U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS (2007), <http://www.justice.gov/oig/special/s0703b/final.pdf>. Critics of the FISA modernization efforts seized upon the misuse of the letters in advocating against increased Executive Branch authority. See, e.g., *Modernization of FISA*, *supra* note 7, at 111 (statement of Caroline Frederickson, American Civil Liberties Union) (“In light of recent revelations that the government is gravely abusing the authorities it already has, allowing this exponential increase in spying authority would not only be unconstitutional, but irresponsible.”).

73. S. REP. NO. 110-209, at 2; see also Foreign Intelligence Surveillance Modernization Act of 2007, H.R. 3782, 110th Cong. (1st Sess. 2007), available at <http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf>. While the government’s submission in April 2007 included numerous proposed revisions, including liability protection provisions for service providers, this Article focuses on the proposed revision to the definition of electronic surveillance.

74. Press Release, U.S. Dep’t of Justice, 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.justice.gov/opa/pr/2007/April/07_nsd_247.html.

75. See S. REP. NO. 111-6, at 2-3 (2008) (reviewing the background of the FISA Amendments Act of 2008 and the Protect America Act of 2007 and indicating that “[o]n May 1, 2007, the Committee [SSCI] held a public hearing to enable the Administration to explain as openly as possible why the legislation it was proposing should be enacted” and that it also held classified hearings); see also *Modernization of FISA*, *supra* note 7, at 1 (statement of Sen. John D. Rockefeller, Chairman, S. Select Comm. on Intelligence) (“The Select Committee on Intelligence meets today in open session, something we don’t often do, to consider whether the scope and application regarding the Surveillance Act needs to change to reflect the evolving needs . . . of foreign intelligence.”).

76. Compare, *Modernization of FISA*, *supra* note 7, at 54-55 (testimony by J. Michael McConnell, Director of National Intelligence & Keith B. Alexander, Director, National Security Agency) (questioning whether the proposed modernizations of FISA would allow intelligence agencies to investigate U.S. persons without obtaining a warrant), with 153 CONG. REC. S10,861 (daily ed. Aug. 3, 2007) (statement of Sen. Feingold) (denouncing the proposed legislation as authorizing “warrantless searches of Americans’ phone calls, e-mails, homes, offices, and personal records”).

(DIRNSA), and the Assistant Attorney General for National Security (AAG) testified in person at the hearing, and experts on national security and civil liberties submitted statements to the Committee.⁷⁷

The DNI argued that the Administration's proposal sought to make FISA "technology neutral" by carving foreign-to-foreign communications of non-U.S. persons out of FISA's definition of electronic surveillance.⁷⁸ At the hearing, the DNI emphasized FISA's preeminent role in this area, noting that when he left the NSA in 1996 FISA's role was "not significant . . . And today it is probably *the* most significant ability we have to target and be successful in preventing attacks."⁷⁹ Administration officials also seized upon the legislative history as demonstrating Congress's reluctance to encroach upon Executive Branch authority.⁸⁰

Critics of the proposal dismissed the effort to update FISA, warning that under the "guise of 'tech neutrality'" the legislation would authorize warrantless surveillance of "virtually all communications in any form by Americans with anyone, including other Americans, located overseas."⁸¹

77. S. REP. NO. 110-209, at 5. For a complete list of the statements for the records at the May 2007 SSCI hearing and the government's proposal, see *Modernization of FISA*, *supra* note 7, at III. This Article generally focuses on the testimony and debate leading up to the enactment of the Protect America Act.

78. *Modernization of FISA*, *supra* note 7, at 18 (testimony by J. Michael McConnell, Director of National Intelligence) ("In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs."). The AAG also focused on FISA's definition of electronic surveillance, arguing that "unanticipated advances in technology [since 1978] have wreaked havoc on the delicate balance that Congress originally struck [in FISA]." *Id.* at 29–30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice). Thus, the government's proposed modification sought to shift the focus from "*how* a communication travels or *where* it is intercepted . . . to *who is the subject of the surveillance.*" *Id.* at 30.

79. *Modernization of FISA*, *supra* note 7, at 48 (testimony by J. Michael McConnell, Director of National Intelligence). The DNI also noted that under the existing statute the Intelligence Community was "often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas. Frequently, although not always, that person's communications are with another foreign person overseas." *Id.* at 11–12 (statement of J. Michael McConnell, Director of National Intelligence); *cf. id.* at 19 ("[T]here were gaps in NSA's coverage of foreign communications and in FBI's coverage of domestic communications." (quoting S. REP. NO. 107-351, at 36 (2002))).

80. For example, Assistant Attorney General Kenneth L. Wainstein has testified that:
Congress recognized the importance of striking an appropriate balance between the need to protect the civil liberties of Americans, and the imperative that the Government be able to collect effectively foreign intelligence information that is vital to the national security. . . . [Congress] also recognized that the terrain in which it was legislating touched upon a core Executive Branch function—the Executive's constitutional responsibility to protect the United States from foreign threats.

Modernization of FISA, *supra* note 7, at 25 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice).

81. *Modernization of FISA*, *supra* note 7, at 187 (statement of Kate Martin, Director, Lisa Graves, Deputy Director, Center for National Security Studies); *see also id.* at 107 (statement of Caroline Frederickson, American Civil Liberties Union) ("Technology may have changed, but the

Another critic dismissed the need to rush to amend FISA, noting that FISA had been amended six times since September 11, 2001.⁸² Despite these and other criticisms, including a general concern that the proposal was “a grasp for spying authority worthy of Big Brother and George Orwell’s *1984*,”⁸³ several supporters and critics of amending FISA alike noted that communications between non-U.S. persons outside the United States are not subject to FISA.⁸⁴

Beginning in late July 2007, the House of Representatives and the Senate considered several bills designed to meet the requirements of the DNI.⁸⁵ Critics expressed concern that the Protect America Act authorized “warrantless searches of Americans’ phone calls,⁸⁶ e-mails, homes, offices

Fourth Amendment has not. Except for a very few circumstances, warrants are required to listen to phone calls or otherwise access the content of a communication . . .”).

82. See *Modernization of FISA*, *supra* note 7, at 99 (statement of Bruce Fein) (“The government has not come close to demonstrating a national security need that would justify the alarming encroachments on the right to be left alone—the liberty most cherished in civilized nations—that would be effectuated by the proposed legislation.”).

83. *Id.*

84. *Id.* at 211 (statement of Suzanne E. Spaulding); *id.* at 130 (statement of David S. Kris); *id.* at 91 (statement of James X. Dempsey, Center for Democracy and Technology).

85. The debate took place at the same time that the Intelligence Community assessed a heightened threat environment. In July 2007, the DNI released the National Intelligence Estimate (NIE) on the Terrorist Threat to the Homeland, assessing that “the US Homeland will face a persistent and evolving terrorist threat over the next three years . . . [primarily] from Islamic terrorist groups and cells, especially al-Qa’ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.” OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, NATIONAL INTELLIGENCE ESTIMATE: THE TERRORIST THREAT TO THE U.S. HOMELAND 5 (2007). The NIE is the DNI’s “most authoritative written judgment concerning national security issues . . . [and] contain[s] coordinated judgments of the Intelligence Community . . .” *Id.* at 1. The DNI also briefed Congress on the threat and the need to amend FISA in late July 2007. See 153 CONG. REC. S10,856 (daily ed. Aug. 3, 2007) (statement of Sen. Kyl) (reporting that the Intelligence Committee of the Senate had been engaged in negotiations with the DNI since he brought the matter to their attention); *id.* at S10858 (statement of Sen. Bond) (recounting that the DNI had submitted proposed reforms to FISA in April 2007 and appeared before a session of the entire Senate in the classified security area in July 2007 to urge immediate reform); S. REP. NO. 110-209, at 5 (2007) (“In late July, the DNI informed Congress that the decision of the second FISA Court judge had led to degraded capabilities in the face of a heightened terrorist threat environment. The DNI urged Congress to act prior to the August recess . . .”).

86. Administration officials later attempted to detail why these concerns were unfounded. See, e.g., *Administration Views of FISA Authorities: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. 46–52 (2007) (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:38878.pdf (reiterating the positions of the Executive Branch regarding many of the concerns and misunderstandings raised by opponents of the Protect America Act); Letter from Alexander W. Joel, Civil Liberties Protection Officer, Office of the Dir. of Nat’l Intelligence, to Silvestre Reyes & Peter Hoekstra, U.S. Reps. (Sept. 17, 2007), available at <http://www.fas.org/irp/news/2007/09/joel091707.pdf> (describing civil liberties and privacy protections contained in the Protect America Act).

and personal records”⁸⁷ with “no court oversight whatsoever.”⁸⁸ Other members expressed concern about turning such power over to the Attorney General.⁸⁹ One member declared that the Protect America Act “eviscerates the Fourth Amendment to the Constitution and represents an unwarranted transfer of power from the courts to the Executive Branch.”⁹⁰

Supporters of the Protect America Act declared “unacceptable” the idea that the government should have to obtain a court order from the FISC when foreign targets communicated overseas.⁹¹ Rather, they supported returning the focus of FISA to protecting the civil liberties of U.S. persons.⁹² Some members supported the Protect America Act due to the ongoing terrorist

87. 153 CONG. REC. S10,864 (daily ed. Aug. 3, 2007) (statement of Sen. Reid). *But see id.* (statement of Sen. Levin) (“[I]f there is an incidental access to U.S. citizens, we obviously will permit that. That is not the problem. It is called minimization.”); 153 CONG. REC. H9,958 (daily ed. Aug. 4, 2007) (statement of Rep. Lungren) (“If, in the capture of this information, we do come into contact with communication that involves someone in the United States, an American citizen, we go through a process called minimization, which means we get it out of there if it has nothing to do with the evil actor.”).

88. 153 CONG. REC. S10,866 (daily ed. Aug. 3, 2007) (statement of Sen. Feingold) (stating that the “clearly erroneous” judicial review standard of the Protect America Act was “basically a standard that is nothing more than a rubberstamp”).

89. *See id.* at H9,688 (statement of Rep. Tierney) (expressing concern that authorizations of surveillance made by the Attorney General would be subject to limited court review with no apparent remedy); *id.* at H9,693 (statement of Speaker Pelosi) (stating that she would not want any attorney general, Republican or Democratic, to have the amount of power given by the Protect America Act). The Protect America Act required certification by both the Attorney General and the DNI. Protect America Act of 2007, Pub. L. No. 110-55, § 105B(a), 121 Stat. 552, 552 (to be codified at 50 U.S.C. § 1805b). Previous versions required only the certification of the Attorney General. *See* 153 CONG. REC. S10,863 (daily ed. Aug. 3, 2007) (statement of Sen. Bond) (pointing out that the requirement for DNI certification was added at the request of Admiral McConnell in light of comments from members of Congress).

90. 153 CONG. REC. H9,957 (daily ed. Aug. 4, 2007) (statement of Rep. Jackson-Lee).

91. *See* 153 CONG. REC. S10,857 (daily ed. Aug. 3, 2007) (statement of Sen. McConnell) (calling the idea that intelligence professionals might have to obtain a FISA warrant in order to conduct overseas surveillance on foreign targets “absolutely absurd and completely unacceptable”). The consensus appeared to be that foreign-to-foreign communications of non-U.S. persons fell outside of FISA. *See, e.g., id.* at S10,866 (statement of Sen. Feingold) (“Not a single Senator doesn’t think we should be able to get at these foreign calls. . . . We simply want protection for the civil liberties of people who have done absolutely nothing wrong.”); *id.* at H9,690 (statement of Rep. Conyers) (“Foreign to foreign does not require a warrant. I don’t know how many times I am going to have to say that.”). One member noted that the FISC itself believed that such matters should not be entertained by the court:

I have a very important message from the DNI: “We understand that the FISA court judges urgently support a more appropriate alignment of the court’s caseload and jurisdiction away from the focus on non-U.S. persons operating outside of the United States. The judges have clearly expressed both frustration with the fact that so much of their docket is consumed by applications that focus on foreign targets and involve minimal privacy interests of Americans.”

See id. at S10,860 (statement of Sen. Bond).

92. *See, e.g., id.* at H9,672–73 (statement of Rep. Wilson) (“We need to go back to what [FISA] was intended to do, which is to protect the civil liberties of Americans and allow us to rapidly collect foreign intelligence on foreign persons in foreign countries without first having to go to court and get a warrant.”).

threat the DNI had described to Congress, the impending congressional recess, and the six-month sunset provision.⁹³

On Friday evening, August 3, 2007, the Senate adopted S. 1927, which had been introduced by Senator McConnell, the ranking minority member, for himself and Senator Bond, the ranking SSCI member, by a vote of 60 to 28.⁹⁴ The efforts of the House of Representatives to pass a competing bill the same evening fell short.⁹⁵ The following evening, August 4, 2007 at 10:19 p.m., the House passed S. 1927 by a vote of 227 to 183.⁹⁶ Highlighting the urgency with which the Administration believed the legislation was needed, as evidenced in the DNI's public statements, President Bush immediately signed the bill on Sunday, August 5, 2007.⁹⁷

B. Statutory Requirements

In an attempt to change FISA to focus on the location of the target instead of the location of the surveillance or the type of communication, the Protect America Act excluded from FISA's definition of electronic surveillance "surveillance directed at a person reasonably believed to be located outside of the United States."⁹⁸ The statute granted the DNI and the Attorney General jointly the authority to "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" for up to one year⁹⁹ and to issue directives to communications service providers requiring them to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition."¹⁰⁰

93. *See id.* at S10,868 (statement of Sen. Feinstein) ("This is not going to be an easy vote for anyone. But what we have to think of right now is, on a temporary basis, how do we best protect the people of the United States against a terrible attack."); *id.* at S10,865 (statement of Sen. Lieberman) ("With all respect to my colleagues, I plead with everyone, let us not strive for perfection. Let us put national security first. Let us understand if this passes . . . we are going to have 6 months to reason together to find something better."). *But see id.* at S10,866 (statement of Sen. Feingold) ("A 6-month sunset does not justify voting for this bad version of the bill. We can't just suspend the Constitution for 6 months.").

94. BAZAN, *supra* note 3, at CRS-1 n.2. At the same time, the Senate also considered a competing bill, S. 2011, introduced by Senator Levin, Chairman of the Armed Forces Committee, on behalf of himself and Senator Rockefeller, the SSCI Chairman. S. 2011, 110th Cong. (2007). S. 2011 did not receive 60 votes, failing 43 to 45. BAZAN, *supra* note 3, at CRS-1 n.3.

95. H.R. 3356, entitled the "Improving Foreign Intelligence Surveillance to Defend the Nations and the Constitution Act of 2007," was introduced by Representative Reyes, the HPSCI Chairman, and Representative Conyers, the House Judiciary Committee Chairman, among others. BAZAN, *supra* note 3, at CRS-1. The vote on the motion to suspend House rules and pass H.R. 3356, which required a two-thirds vote instead of a majority, was 218 to 207. *Id.* at CRS-1 n.4.

96. *Id.* at CRS-1 n.5.

97. *Id.* at CRS-1.

98. Protect America Act of 2007, Pub. L. No. 110-55, § 105A, 121 Stat. 552, 552 (to be codified at 50 U.S.C. § 1805a).

99. *Id.*

100. *Id.*

To guarantee that acquisition only targeted persons outside the United States and to protect the privacy of U.S. persons, the Protect America Act required that the DNI and Attorney General certify that:

- (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to [the Protect America Act];
- (2) the acquisition does not constitute electronic surveillance;
- (3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person . . . who has access to communications, either as they are transmitted or while they are stored . . . ;
- (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
- (5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section [1801(h) of FISA].¹⁰¹

The certification, however, was not required to “identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.”¹⁰² The procedures were subject to the FISC’s review under a clearly erroneous standard.¹⁰³

Moreover, where a communications service provider failed to comply with a lawful directive, the Protect America Act authorized the Attorney General to move to compel compliance with the directive before the FISC.¹⁰⁴ The statute also permitted the recipient of a directive to challenge its legality before the FISC and, if the FISC did not deem the petition frivolous upon initial review, the FISC could modify or set aside the directive if the judge found that the directive did not meet the requirements of the statute or was otherwise unlawful.¹⁰⁵

101. *Id.* § 105B(a). The same section required that the certification, relying as appropriate upon affidavits of national security officials, be in writing unless immediate action was required and time did not permit the preparation of a written certification. *Id.*

102. *Id.* § 105B(b).

103. *Id.* § 105C.

104. *Id.* § 105B(g).

105. *Id.* §§ 105B(h)(1)(A)–(B). As originally enacted, portions of the Protect America Act were scheduled to sunset 180 days from the date of enactment. ELIZABETH B. BAZAN, CONG. RESEARCH SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: COMPARISON OF THE SENATE AMENDMENT TO H.R. 3773 AND THE HOUSE AMENDMENT TO THE SENATE AMENDMENT TO H.R. 3773, at 2 (2008). Congress later passed a fifteen-day extension of the Protect America Act, so those portions did not expire until February 16, 2008. *Id.* Congress subsequently enacted the FISA Amendments Act of 2008, which President Bush signed on July 10, 2008. President George W. Bush, President Bush Signs H.R. 6304, FISA Amendments Act of 2008 (July 10, 2008) (transcript available at <http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/>)

IV. The Court of Review Decision

The Court of Review in *In re Directives* did not write on a blank slate. Indeed, the decision is consistent with legal precedent regarding the Executive Branch's acquisition of foreign intelligence information in a manner consistent with the requirements of the Fourth Amendment.¹⁰⁶ First, the Court of Review held that a foreign intelligence exception to the Warrant Clause exists, at a minimum, in the limited circumstances outlined below.¹⁰⁷ Second, the court held that the warrantless surveillance comports with the Fourth Amendment's reasonableness requirement, even where the surveillance acquires communications of a U.S. person who is not a target of the surveillance.¹⁰⁸ The two holdings are significant for their clarity and because they answered constitutional questions regarding the Executive Branch's authority to conduct certain surveillance without prior judicial review so soon after that very issue was debated before Congress.

A. *The Directives and a Summary of the Provider's Challenge*

In 2007, the government issued directives to the provider.¹⁰⁹ The directives required the provider to assist the government in its acquisition of foreign intelligence information through the warrantless surveillance of certain of the provider's customers reasonably believed to be located outside the United States.¹¹⁰

The directives were issued pursuant to Protect America Act certifications.¹¹¹ At least on the face of the statute, the directives lacked key attributes of a traditional warrant. They were issued without a particularity requirement and a requirement for prior judicial review for determining probable cause.¹¹² Those certifications, however, contained protections beyond those specified by the statute, namely the requirement that the Attorney

20080710-2.html). For a discussion of congressional action between August 2007 and July 2008, see generally BAZAN, *supra*.

106. See *infra* notes 132–36 and accompanying text.

107. See *In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (“[W]e hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.”).

108. *Id.* at 1013, 1015.

109. *Id.* at 1007.

110. *Id.* at 1006–07.

111. *Id.* at 1007.

112. See *id.* at 1013–14 (noting that the Protect America Act lacks a particularity requirement and a prior judicial review requirement for determining probable cause, protections equivalent to the principal warrant requirements); Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805a, 1805b) (listing the requirements to which the DNI and Attorney General must certify as well as indicating that the DNI and Attorney General may direct a person to “immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition”). For a fuller discussion of the Court of Review’s consideration of prior judicial review, see *infra* text accompanying notes 196–209.

General and the NSA follow procedures implemented pursuant to § 2.5 of Executive Order 12,333, as amended.¹¹³ Section 2.5 of Executive Order 12,333 provides that the Attorney General may authorize surveillance of U.S. persons only when the Attorney General has “determined in each case that there is probable cause to believe that the [surveillance] technique is directed against a foreign power or an agent of a foreign power.”¹¹⁴ In addition, the certifications contained procedures designed to direct any authorized surveillance against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.¹¹⁵

The provider refused to comply with the directives.¹¹⁶ Pursuant to § 105B(g) of the Protect America Act, the Government moved the FISC for an order compelling the provider’s compliance.¹¹⁷ After “amplitudinous” briefing, the FISC issued a “meticulous” opinion validating the directives and granting the motion to compel.¹¹⁸ The provider then filed a petition for review with the Court of Review and moved the FISC for a stay pending its appeal.¹¹⁹ When the FISC denied the motion for a stay and threatened to hold the provider in civil contempt, the provider began compliance with the directives.¹²⁰

The provider continued to comply throughout the proceedings before the Court of Review.¹²¹ On August 22, 2008, following oral argument on the merits, the Court of Review issued a classified opinion that affirmed the FISC’s decision that the directives were lawful and that compliance was

113. *In re Directives*, 551 F.3d at 1007. Because the Protect America Act did not distinguish between U.S. persons and non-U.S. persons, the government was being more restrictive than the statute by applying § 2.5 to the certifications. *See supra* note 60 (indicating that § 2.5 authorized surveillance only “within the United States or against a United States person abroad”); *infra* text accompanying note 126 (relating that the Protect America Act authorized surveillance of persons reasonably believed to be outside the United States, without regard to U.S.-person status).

114. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended in* 50 U.S.C. § 401 (2006).

115. *In re Directives*, 551 F.3d at 1007–08. The FISC found the government’s procedures implementing the statute sufficient under the Protect America Act. *See* NSD PROGRESS REPORT, *supra* note 66, at 21 (“On January 15, 2008, the FISA Court, after reviewing the Government’s submissions, issued an order upholding the procedures the Government uses to determine that targets subject to surveillance under this authority are reasonably believed to be abroad.”); *see also In re Directives*, 551 F.3d at 1015 (noting that “[t]hese minimization procedures were upheld by the FISC in this case”).

116. *In re Directives*, 551 F.3d at 1008.

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.* The provider also moved the Court of Review for a stay pending appeal. *Id.* The Court of Review reserved decision on the motion for a stay, and the provider continued its compliance with the directives. *Id.* As part of its opinion upholding the lawfulness of the directives, the Court of Review denied the motion for a stay as moot. *Id.* at 1016.

121. *Id.* at 1008.

required.¹²² By order dated January 12, 2009, the Court of Review issued a redacted, unclassified version of its opinion.¹²³

B. The Limited Scope of the Fourth Amendment Claim

The provider's Fourth Amendment arguments were limited in terms of the persons whose interests it sought to vindicate.¹²⁴ The provider challenged the directives only in regard to the Fourth Amendment rights of U.S. persons.¹²⁵ The statute, however, had a broader application. The statute authorized surveillance of persons reasonably believed to be outside the United States, without regard to U.S.-person status.¹²⁶ To the extent targets were non-U.S. persons, however, the statute and any directives thereunder did not implicate the Fourth Amendment because the Fourth Amendment does not apply to searches of non-U.S. persons located outside the United States.¹²⁷ The constitutional challenge accordingly focused on the Fourth Amendment rights of two categories of U.S. persons: U.S. persons abroad who were the targets of surveillance and U.S. persons whose

122. *Id.* at 1004, 1008, 1016.

123. *Id.* at 1016–18.

124. Before reaching the merits of the Fourth Amendment claim, the Court of Review addressed the Government's argument that the provider lacked standing to challenge the legality of the directives on behalf of its customers. Specifically, the Government had argued that the provider's claim was contrary to the rule that a litigant cannot bring suit to vindicate the rights of third parties. *See id.* at 1008 (citing *Hinck v. United States*, 550 U.S. 501, 510 n.3 (2007), and *Warth v. Seldin*, 422 U.S. 490, 499 (1975), for the rule that a litigant must assert his own legal rights, not those of third parties); *see also* *Cal. Bankers Ass'n v. Schultz*, 416 U.S. 21, 69–70 (1974) (refusing to consider a bank's claim that certain federal reporting requirements violated the Fourth Amendment rights of non-party bank customers "whose transactions must be reported" under federal law); *Alderman v. United States*, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted."); *Hollingsworth v. Hill*, 110 F.3d 733, 738 (10th Cir. 1997) (holding that a mother could not challenge seizure of her minor children on the ground that it violated her children's Fourth Amendment rights because her complaint did not include the children as plaintiffs); *Ellwest Stereo Theatres, Inc. v. Wenner*, 681 F.2d 1243, 1248 (9th Cir. 1982) (rejecting an adult theater's challenge to a city ordinance on the ground that any police surveillance enabled by the ordinance did not threaten the theater's Fourth Amendment interests, but only "the interests of its patrons"). The Court of Review held that the provider "easily exceed[ed] the constitutional threshold for standing." *In re Directives*, 551 F.3d at 1008. Furthermore, it held that any prudential standing limitation was relaxed by the terms of the Protect America Act, which expressly placed no limits on the types of claims a provider could bring. *See id.* at 1008–09 ("We think that the language is broad enough to permit a service provider to bring a constitutional challenge to the legality of a directive regardless of whether the provider or one of its customers suffers the infringement that makes the directive unlawful.")

125. *In re Directives*, 551 F.3d at 1009.

126. Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805a, 1805b).

127. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) (holding that only those persons who "have come within the territory of the United States and developed substantial connections" with the country have Fourth Amendment rights).

communications were collected incidentally by the government while targeting individuals abroad.¹²⁸

In the context of these limits, the provider advanced two Fourth Amendment arguments. First, it argued that the Fourth Amendment's Warrant Clause applied to the surveillance and that the directives were unlawful because they were not warrants.¹²⁹ Second, the provider argued that even if the Warrant Clause did not apply, the surveillance failed to satisfy the Fourth Amendment's reasonableness requirement.¹³⁰ The court rejected each of these arguments.¹³¹

1. A Clear Holding: Foreign Intelligence Collection Is a Special Need Excusing Compliance with the Warrant Clause.—Prior case law provided little support for the provider's argument that the Warrant Clause applied to the type of foreign intelligence surveillance authorized by the Protect America Act. Every court of appeals to decide the question had held that the Fourth Amendment does not require the government to obtain a judicial warrant before conducting a foreign intelligence search.¹³² Many, if not all, of

128. See *In re Directives*, 551 F.3d at 1009 (relating that the petitioner's claims were limited to the harm that may be inflicted upon U.S. persons); *id.* at 1014 (explaining that § 2.5 of Executive Order 12,333, which the government applied to the certifications, authorizes surveillance "within the United States or against a United States person abroad"); *id.* at 1015 (referencing the implemented minimization procedures, which aimed at "reducing the impact of incidental intrusions into the privacy of non-targeted United States persons"). The Court of Review also limited its analysis of the claim to the particularized fact record before it. *Id.* at 1010. The provider had argued that its challenge was a facial challenge to the statute. *Id.* at 1009. Under a facial challenge analysis, a court considers the constitutionality of a statute without regard to facts describing the government's particular application of the statute. *Id.* The Court of Review held that the challenge, in fact, was an as-applied challenge and not a facial challenge. *Id.* at 1009–10. There was a particularized record, the statute was applied to the provider in a specific setting, and the provider's arguments took account of that setting. *Id.* at 1009. "So viewed, [the arguments] go past the question of whether the [Protect America Act] is valid on its face—a question that would be answered by deciding whether *any* application of the statute passed constitutional muster . . .—and ask instead whether this specific application offends the Constitution." *Id.* at 1009–10 (citing *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449 (2008)). Because the court conducted an as-applied analysis, it considered, among other things, the extra-statutory privacy protections implemented through the certifications and directives. See *In re Directives*, 551 F.3d at 1013–14 (considering the Protect America Act as applied here, including "the protections spelled out in the [Act] itself and those mandated under the certifications and directives").

129. *In re Directives*, 551 F.3d at 1009.

130. *Id.*

131. *Id.* at 1010–12.

132. See *United States v. Truong Dinh Hung*, 629 F.2d 908, 912–16 (4th Cir. 1980) (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement . . ."); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (upholding warrantless foreign intelligence surveillance and relying on the "good faith of the Executive and the sanctions for illegal surveillances incident to post-search criminal or civil litigation"); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) ("[B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence.");

these cases involved surveillance inside the United States.¹³³ If, as they held, there was an exception to the Warrant Clause for the collection of foreign intelligence information from persons inside the United States, then this foreign intelligence exception applied *a fortiori* to acquisitions pursuant to the Protect America Act that were directed at persons reasonably believed to be outside the United States.

The Court of Review, in *In re Sealed Case*,¹³⁴ itself recognized a foreign intelligence exception to the warrant requirement.¹³⁵ In that case, the Court of Review held that surveillance for foreign intelligence information under FISA complied with the Fourth Amendment without determining whether an electronic surveillance order under 50 U.S.C. § 1805 constituted a “warrant” within the meaning of the Warrant Clause.¹³⁶ Although it avoided an express holding that a foreign intelligence exception exists, such a holding was implicit: had the Warrant Clause applied, the Court of Review would have had to have determined whether a FISA electronic surveillance order was a warrant. Because it upheld the lawfulness of the electronic surveillance order on Fourth Amendment reasonableness grounds without the warrant determination, the court implicitly held that no warrant was required.¹³⁷

In *In re Directives*, however, the court’s holding was express:

[W]e hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when the surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.¹³⁸

see also In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (“[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.”). In *Zweibon v. Mitchell*, 516 F.2d 594, 633–51 (D.C. Cir. 1975) (en banc) (plurality opinion), a plurality of the D.C. Circuit suggested that a warrant might be required to conduct surveillance for foreign intelligence purposes, but this suggestion was dicta. *See In re Sealed Case*, 310 F.3d at 742 n.26 (noting that in regard to a foreign intelligence exception to the warrant requirement, *Zweibon* “suggested the contrary in dicta, it did not decide the issue”).

133. *See, e.g., Truong*, 629 F.2d at 912 (involving eavesdropping on telephone conversations and bugging an apartment in the United States); *Buck*, 548 F.2d at 874 (relating to electronic surveillance in the United States); *Butenko*, 494 F.2d at 596 (discussing “the relationship between the federal government’s need to accumulate information concerning activities within the United States of foreign powers and the people’s right of privacy as embodied in the Fourth Amendment”); *Brown*, 484 F.2d at 426 (concluding that wiretaps conducted in the United States were lawful).

134. 310 F.3d at 717.

135. *Id.* at 741–42.

136. *Id.* at 742.

137. *See id.* at 741–42 (noting that “a FISA order may not be a ‘warrant’ contemplated by the Fourth Amendment” and remarking that the “government itself does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense”).

138. *In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

The court, furthermore, based its holding on Fourth Amendment principles developed outside the context of foreign intelligence surveillance.¹³⁹

Although the Supreme Court had not expressly recognized an exception to the Warrant Clause for foreign intelligence surveillance,¹⁴⁰ it had issued a relevant body of decisions referred to as “special needs” cases.¹⁴¹ As the Court of Review noted, those cases “excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.”¹⁴² The Court of Review held that the reasoning of the special needs cases applied to justify an exception to the warrant requirement for surveillance pursuant to the Protect America Act.¹⁴³

The threshold consideration in the special needs cases is whether a search was designed to uncover evidence of “ordinary criminal wrongdoing” or was motivated “at [a] programmatic level” by other governmental objectives.¹⁴⁴ The Court of Review held that Protect America Act

139. *Id.* at 1010–12.

140. The Supreme Court in *Keith* expressly reserved the question of whether the Fourth Amendment required a warrant for foreign intelligence surveillance, but in so doing suggested possible parameters for such an exception. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 321–22 (1972) (“As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues that may be involved with respect to activities of foreign powers or their agents.”). In concluding that the Fourth Amendment’s warrant requirement applies to investigation of purely domestic threats to security, the *Keith* Court discussed several sources supporting “the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved.” *Id.* at 322 n.20; *see also Katz v. United States*, 389 U.S. 347, 358 n.23 (1967) (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”).

141. *In re Directives*, 551 F.3d at 1010.

142. *Id.* (citations omitted).

143. *Id.* at 1011.

144. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37–40, 48 (2000); *see also In re Directives*, 551 F.3d at 1011 (“In our view the more appropriate consideration is the programmatic purpose of the surveillances and whether—as in the special needs cases—that programmatic purpose involves some legitimate objective beyond ordinary crime control.”). Accordingly, the Supreme Court has permitted, *inter alia*, the following: warrantless stops of motorists at roadblocks for the purpose of securing the border, *see United States v. Martinez-Fuerte*, 428 U.S. 543, 566 (1976) (holding that vehicle stops at fixed checkpoints for brief questioning of the occupants, even though there is not reason to believe a particular vehicle contains illegal aliens, are consistent with the Fourth Amendment and need not be authorized by warrant); warrantless searches of the homes of persons on probation to ensure compliance with probation conditions, *see Griffin v. Wisconsin*, 483 U.S. 866, 872–73 (1987) (holding that the search of a home satisfied the demands of the Fourth Amendment because it was carried out pursuant to a regulation that itself satisfied the Fourth Amendment’s reasonableness requirement); and warrantless searches of public school students in order to enforce school rules, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that the “fundamental command of the Fourth Amendment is that searches and seizures be reasonable, and although ‘both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search, . . . in certain limited circumstances neither is required’”). The Supreme Court has also approved warrantless and suspicionless drug testing of the following groups: students

surveillances had a programmatic purpose “well beyond any garden-variety law enforcement objective,” and “easily pass muster” in this regard.¹⁴⁵ This conclusion was consistent with the decision in *In re Sealed Case*.¹⁴⁶ The programmatic purpose of surveillance approved in that case was fundamentally the same as the programmatic purpose of surveillance authorized by the directives: the acquisition of foreign intelligence information to protect against threats to national security directed by foreign powers and their agents.¹⁴⁷ In support of this conclusion, the Court of Review found that the “stated purpose” of the directives “centers on garnering foreign intelligence.”¹⁴⁸ The court also observed that there was “no indication that

involved in extracurricular activities, *see* *Bd. of Educ. v. Earls*, 536 U.S. 822, 829–38 (2002) (holding that a policy requiring all students who participate in competitive extracurricular activities submit to drug testing was a reasonable means of furthering the school district’s interest in thwarting and discouraging drug use among students and therefore did not violate the Fourth Amendment); students involved in school athletics, *see* *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 664–65 (1995) (upholding drug testing of high school athletes and explaining that the exception to the warrant requirement applied when special needs that are beyond the normal need for law enforcement make the warrant and probable cause requirements unworkable); federal employees charged with enforcing drug laws or carrying firearms, *see* *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 679 (1989) (holding that when the government requires its employees to produce urine samples to be analyzed for illegal drug use, the collection and analysis of such samples are searches that meet the reasonableness requirement of the Fourth Amendment); and railroad employees whose job functions implicate safety concerns, *see* *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 624 (1989) (upholding regulations instituting drug and alcohol testing of railroad workers for safety reasons).

145. *In re Directives*, 551 F.3d at 1011.

146. Courts in similar cases have held that searches to protect against threats to national security qualify for the special needs exception to the warrant requirement. *See* *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (“[T]he prevention of terrorist attacks . . . constitutes a ‘special need’ Preventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them.”); *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006) (“[P]reventing a terrorist from bombing the subways constitutes a special need that is distinct from ordinary post hoc criminal investigation.”).

147. *Compare In re Directives*, 551 F.3d at 1011 (finding that surveillances authorized by directives involve “the acquisition from overseas agents of foreign intelligence to help protect national security”), *with In re Sealed Case*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (holding that the programmatic purpose was “to protect the nation against terrorists and espionage threats directed by foreign powers”).

148. *In re Directives*, 551 F.3d at 1011. The debate regarding the Protect America Act included concerns that, without more oversight, the government would use the statute’s authorities for purposes other than those authorized by the statute. *See Modernization of FISA*, *supra* note 7, at 44 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice). The Court of Review did not entertain such arguments, instead presuming that the government acted as it stated. *See In re Directives*, 551 F.3d at 1011 (“Without something more than a purely speculative set of imaginings, we cannot infer that the purpose of the directives (and, thus, of the surveillances) is other than their stated purpose.”). *See, e.g., United States v. Chem. Found., Inc.*, 272 U.S. 1, 14–15 (1926) (“The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.” (internal citations omitted)).

the collections of information [were] primarily related to ordinary criminal-law enforcement purposes.”¹⁴⁹

Next, the Court of Review held that that the Protect America Act surveillance satisfied the second consideration for a special needs exception: a warrant requirement would “materially interfere with the accomplishment of” the programmatic purpose.¹⁵⁰ The Government’s proof on this point was bolstered by congressional findings.¹⁵¹ Congress passed the Protect America Act precisely because the burden of preparing FISA applications was harming the government’s ability to collect foreign intelligence information from targets overseas.¹⁵² Citing classified information that was redacted from the published opinion and not given to the provider in the litigation, the court held that “there is a high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.”¹⁵³ In addition, the court held that “[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government’s ability to collect information in a timely manner.”¹⁵⁴

2. *Warrantless Collection of U.S.-Person Communications Is Reasonable Under the Fourth Amendment.*—Although the Government established a special-needs exception to the Warrant Clause for its foreign intelligence surveillance, the Fourth Amendment still required that the surveillance be reasonable. As the Court of Review noted, “the question here

149. *In re Directives*, 551 F.3d at 1011. The provider argued that the government could not invoke a foreign intelligence exception unless the primary purpose of the search was the collection of foreign intelligence. The Court of Review, however, had rejected the “primary purpose” test in *In re Sealed Case* as being inconsistent with special needs case law and its programmatic purpose analysis. Citing its holding in *In re Sealed Case*, the Court of Review rejected the provider’s argument on the same grounds. *See id.* (“That dog will not hunt.”).

150. *Id.* at 1010.

151. *Id.* at 1008–09.

152. *See, e.g.*, 153 CONG. REC. S10,857 (daily ed. Aug. 3, 2007) (statement of Sen. McConnell) (stating that the legislation’s purpose is to provide the government with “the speed and the flexibility” to “collect foreign intelligence concerning foreign targets overseas in another country”).

153. *In re Directives*, 551 F.3d at 1011 (citations omitted). In describing the compelling needs of the Executive in foreign intelligence gathering, the *Truong* court observed,

[A]ttempts to counter foreign threats to the national security require utmost stealth, speed, and secrecy. A warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.

United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); *see also* *United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000) (finding that “the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden” on the government’s ability to obtain foreign intelligence information effectively); *cf. In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 171 (2d Cir. 2008) (“[W]e hold that the Fourth Amendment’s Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment’s requirement of reasonableness.”).

154. *In re Directives*, 551 F.3d at 1011–12.

reduces to whether the [statute], as applied through the directives, constitutes a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment.”¹⁵⁵

In evaluating reasonableness, the Court of Review invoked well-settled Fourth Amendment standards. Reasonableness would be determined based on the totality of the circumstances, balancing the interests at stake.¹⁵⁶ This analysis would account for the nature of the government intrusion and how the intrusion is implemented.¹⁵⁷ The greater the government interest, the greater the intrusion that may be tolerated.¹⁵⁸ If, based on these considerations, “the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake,” the court would uphold the surveillance as constitutional.¹⁵⁹ If, however, “those protections are insufficient to alleviate the risks of government error and abuse,” the court would find the surveillance to be unconstitutional.¹⁶⁰

In terms of the government’s interest in the surveillance, there was little debate: the government had put forth an interest “of the highest order of magnitude,” the interest in national security.¹⁶¹ Under the reasonableness standards set forth by the Court of Review, this “important interest” in national security could justify a greater intrusion in individual privacy.¹⁶² But before it considered the relative merits of those protections, the court revisited its *In re Sealed Case* decision to respond to the provider’s arguments about what *In re Sealed Case* did and did not say about the application of the totality-of-circumstances test and the reasonableness of foreign intelligence surveillance.¹⁶³

The provider argued that the totality-of-circumstances test required consideration of certain specific factors.¹⁶⁴ It first argued that the court must consider the six factors that *In re Sealed Case* found contributed to the protection of individual privacy in the face of government intrusion for national security purposes—prior judicial review, presence or absence of probable cause, particularity, necessity, limited duration, and minimization.¹⁶⁵ As a related point, the provider next argued that *In re*

155. *Id.* at 1012.

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.* at 1012 (citing *Haig v. Agee*, 453 U.S. 280, 307 (1981) (“It is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” (internal citations omitted)) and *In re Sealed Case*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (holding that the national security threat at issue “may well involve the most serious threat our country faces”)).

162. *Id.* at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701–05 (1981)).

163. *Id.* at 1012–13.

164. *Id.* at 1012.

165. *Id.*

Sealed Case required that surveillance pursuant to the directives must contain procedures equivalent to the three principal warrant requirements, namely prior judicial review, probable cause, and particularity.¹⁶⁶

The Court of Review summarily rejected these arguments. It held that *In re Sealed Case* did not formulate a “rigid six-factor test for reasonableness.”¹⁶⁷ Such a test “would be at odds with the totality of the circumstances test,”¹⁶⁸ and, in any event, *In re Sealed Case* “merely indicated that the six enumerated factors were relevant under the circumstances of that case.”¹⁶⁹

In re Sealed Case was clear on this point: the procedures it considered in evaluating the reasonableness of FISA surveillance—procedures required by Title III for ordinary criminal warrants—were “not constitutionally required.”¹⁷⁰ The Court of Review looked instead to such procedures as “instructive” to its reasonableness analysis, recognizing that reasonableness depends on the “facts and circumstances of each case.”¹⁷¹ Given FISA’s resemblance to a traditional warrant regime, it made sense for the Court of Review in *In re Sealed Case* to compare FISA to the Title III procedures in assessing reasonableness.¹⁷² But the Court of Review did not hold that such procedures were constitutionally required. Rather, it weighed such procedures, among many other factors, in its assessment of the reasonableness of the FISC orders under the Fourth Amendment.¹⁷³

The Court of Review also rejected the provider’s argument that directives must contain protections equivalent to the three principal warrant clause requirements of prior judicial review, probable cause, and particularity.¹⁷⁴ This argument, the court held, was essentially an attempt to impose a warrant requirement on foreign intelligence surveillance that it had determined was exempt from just such a requirement.¹⁷⁵ The argument also misread *In re Sealed Case*. These three warrant requirements were relevant to a reasonableness analysis—“the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds”—but they

166. *Id.* at 1013.

167. *Id.* at 1012.

168. *Id.* at 1012–13. Indeed, the determination whether a search is reasonable “requires careful attention to the facts and circumstances of each particular case.” *Graham v. Connor*, 490 U.S. 386, 396 (1989); *see also* *United States v. Redmon*, 138 F.3d 1109, 1128 (7th Cir. 1998) (Flaum, J., concurring) (“No one factor can be a talismanic indicator of reasonableness . . .”).

169. *In re Directives*, 551 F.3d at 1013.

170. *In re Sealed Case*, 310 F.3d 717, 737 (FISA Ct. Rev. 2002).

171. *Id.* at 737, 740.

172. *See id.* at 737–42 (detailing the similarities between FISA and Title III and noting that how closely a FISA order complies with Title III bears on the reasonableness analysis under the Fourth Amendment).

173. *Id.*

174. *In re Directives*, 551 F.3d at 1013.

175. *Id.*

were not of themselves determinative.¹⁷⁶ Consistent with Fourth Amendment case law, the guiding principle would be the totality of the circumstances, and not some limited set of circumstances.¹⁷⁷

Based on the totality of circumstances, the Court of Review held that the directives constituted reasonable government action.¹⁷⁸ The Protect America Act, the certifications, and the directives contained a “matrix of safeguards.”¹⁷⁹ The provider offered only a “parade of horrors” concerning these safeguards, but no evidence that, notwithstanding the safeguards, there was “any actual harm, any egregious risk of error, or any broad potential for abuse”¹⁸⁰ Thus, in light of the important government interest in national security and the “panoply of protections,” the court held that there was “no principled basis for invalidating the [Protect America Act] as applied here.”¹⁸¹

To reach its reasonableness conclusion, the Court of Review focused on the issues of particularity, probable cause, prior judicial review, and the incidental collection of information from non-targeted U.S. persons.¹⁸² With respect to particularity, the Protect America Act did not require a showing of particularity.¹⁸³ Although required by the Warrant Clause,¹⁸⁴ particularity in the context of warrantless searches is but one factor among many in assessing reasonableness.¹⁸⁵ The Court of Review held that the surveillance authorized by the directives sufficiently addressed any particularity considerations.¹⁸⁶ It did so by analogy to FISA electronic surveillance, which it had held was reasonable in *In re Sealed Case*.¹⁸⁷ FISA’s electronic surveillance provisions require probable cause to believe that the facility or place at which surveillance is directed is being used, or about to be used, by an agent of a foreign power.¹⁸⁸ In the case before it, the Court of Review found that

176. *See id.* (declining to incorporate warrant requirements into the foreign intelligence exception of the Fourth Amendment).

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.* at 1013–14.

183. *Id.* at 1013 (citing 50 U.S.C. § 1805b(b) (Supp. I 2007–2008)).

184. *See* U.S. CONST. amend. IV (“[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched*.” (emphasis added)).

185. *See* *United States v. Martinez-Fuerte*, 428 U.S. 543, 561 (1976) (proclaiming that “the Fourth Amendment imposes no irreducible requirement” of individualized findings where the search in question is otherwise reasonable).

186. *In re Directives*, 551 F.3d at 1013–14.

187. *Id.*

188. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 104, 92 Stat. 1783, 1789 (codified at 50 U.S.C. § 1805(a)(3)(B) (2006)).

certain classified procedures were “analogous to and in conformity with the particularity showing contemplated by *Sealed Case*.”¹⁸⁹

The Court of Review held that any probable cause concern was allayed by the Attorney General’s findings made pursuant to § 2.5 of Executive Order 12,333, made applicable to the surveillances through the certifications and directives.¹⁹⁰ Section 2.5 authorizes the Attorney General to approve “the use for intelligence purposes . . . against a U.S. person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes”¹⁹¹ The Attorney General may authorize such surveillance only when he “determine[s] in each case that there is *probable cause* to believe that the [surveillance] technique is directed against *a foreign power or an agent of a foreign power*.”¹⁹² As applied to Protect America Act surveillance, the court found that, before the government could act upon the certifications, the Attorney General must determine that there was probable cause to believe that the targeted U.S. person was a foreign power or agent of a foreign power.¹⁹³ This determination was supported by, among other information, a several-page statement of facts provided by the NSA in support of the probable cause determination.¹⁹⁴

Harkening back to the debate concerning the Protect America Act,¹⁹⁵ the provider also argued that the directives were unreasonable because, without prior judicial review, they “cede to [the Executive] Branch overly broad power that invites abuse.”¹⁹⁶ The Court of Review described this argument as “little more than a lament about the risk that government officials will not operate in good faith.”¹⁹⁷ A prior judicial review requirement does not eliminate that risk—it “exists even when a warrant is required.”¹⁹⁸ Despite the risk of fraud or misconduct by a warrant affiant, courts traditionally apply a presumption of regularity to the obtaining of a warrant, unless there is a showing of actual fraud or misconduct.¹⁹⁹ In the same way, the Court of Review applied a presumption of regularity to the Executive Branch’s decision to authorize surveillance.²⁰⁰ It analyzed whether the government

189. See *In re Directives*, 551 F.3d at 1013–14 (noting that the classified procedures were part of an ex parte appendix filed by the Government and not disclosed to petitioner).

190. *Id.* at 1014.

191. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981).

192. *Id.* (emphasis added).

193. *In re Directives*, 551 F.3d at 1014.

194. *Id.* at 1014 n.7; see also *supra* note 60.

195. See 153 CONG. REC. H9,957 (daily ed. Aug. 4, 2007) (statement of Rep. Jackson-Lee) (lamenting the Protect America Act’s “unwarranted transfer of power from the courts to the Executive Branch”).

196. *In re Directives*, 551 F.3d at 1014.

197. *Id.*

198. *Id.*

199. *Id.*

200. See *id.* (“Here—where an exception affords relief from the warrant requirement—common sense suggests that we import the same presumption.”).

had put in place protections and procedures sufficient to satisfy the Fourth Amendment's reasonableness requirement.²⁰¹ Once the Court of Review determined that those protections and procedures were sufficient, it would not assume that the government would implement them in bad faith, absent evidence to that effect.²⁰²

The court had applied the same presumption of regularity when evaluating the government's programmatic purpose for a special-needs exception to the Warrant Clause. In that context, the provider's "purely speculative set of imaginings" were no basis to question the government's stated, programmatic purpose.²⁰³ Likewise, in the context of evaluating the Fourth Amendment reasonableness of the government's procedures, the provider's "parade of horrors" did not undermine otherwise reasonable procedures.²⁰⁴

Prior judicial review, moreover, did not ensure against the risk of inadvertent collection, and in general, the "potential for error is not a sufficient reason to invalidate the surveillances."²⁰⁵ The court noted that the government had put in place "effective minimization procedures" that serve as "an additional backstop against identification errors."²⁰⁶ Those minimization procedures were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," were approved by the FISC in the case below,²⁰⁷ and were approved in the FISA context by the Court of Review in *In re Sealed Case*.²⁰⁸ The court, accordingly, held that it saw "no reason to question the adequacy of the minimization protocol."²⁰⁹

The court also addressed the provider's arguments regarding the incidental collection of U.S. person communications—that is, the collection of communications of U.S. persons who are not targeted for surveillance but who are in communication with targeted persons reasonably believed to be located outside the United States.²¹⁰ This holding goes to the heart of the debate on the Protect America Act. As noted above, even critics of the Protect America Act did not dispute that FISA should not cover foreign-to-foreign communications by non-U.S. persons.²¹¹ Rather, they were concerned about the collection of U.S.-person communications being sucked up

201. *Id.* at 1014–15.

202. *Id.*

203. *Id.* at 1011.

204. *Id.* at 1013.

205. *Id.* at 1014–15; *see also* *Pasiewicz v. Lake County Forest Pres. Dist.*, 270 F.3d 520, 525 (7th Cir. 2001) ("[T]he Fourth Amendment demands reasonableness, not perfection.").

206. *In re Directives*, 551 F.3d at 1015.

207. *Id.*

208. 310 F.2d 717, 731 (FISA Ct. Rev. 2002).

209. *In re Directives*, 551 F.3d at 1015.

210. *Id.*

211. *See supra* notes 83–84 and accompanying text.

in NSA's so-called "vacuum cleaner."²¹² The court held that the provider's "concern with incidental collections is overblown."²¹³ According to the Court of Review, "[i]t is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."²¹⁴ This conclusion applies fully to surveillance for the purpose of collecting foreign intelligence.²¹⁵

The directives, in any event, extended certain protections to U.S. persons whose communications were incidentally collected. The Court of Review noted two such protections in particular: targeting procedures and minimization procedures.²¹⁶ The targeting procedures "include provisions to prevent errors" and the Protect America Act provides for both Executive Branch and congressional oversight of compliance with the targeting procedures.²¹⁷ Minimization procedures, which the court described as "effective," also protected those impacted by incidental collection.²¹⁸ As noted by the court, minimization procedures serve "as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."²¹⁹ Together, these protections for U.S. persons whose

212. James X. Dempsey of the Center for Democracy Technology (CDT) stated to Congress that the term "vacuum cleaner" was appropriate because the Protect America Act "would permit [the NSA] without a warrant the untargeted collection of many, many calls, without the particularized suspicion required by the Constitution for government searches," but also added that "the CDT has been on the record supporting an amendment to FISA that would make it clear that a warrant is not needed when the government is intercepting foreign-to-foreign communications that happen to be available in the U.S." *Modernization of FISA*, *supra* note 7, at 88–91 (statement of James X. Dempsey, Policy Director, Center for Democracy and Technology).

213. *In re Directives*, 551 F.3d at 1015; *see also supra* note 87 (statement of Sen. Levin).

214. *In re Directives*, 551 F.3d at 1015 (citing *United States v. Kahn*, 415 U.S. 143, 157–58 (1974) (holding that the interception of a wife's communications incident to the lawful wiretap of a home phone targeting her husband's communications did not violate the Fourth Amendment) and *United States v. Schwartz*, 535 F.2d 160, 164 (2d Cir. 1976) ("It is virtually impossible to completely exclude all irrelevant matter from intercepted conversations."); *see also* *United States v. Figueroa*, 757 F.2d 466, 472–73 (2d Cir. 1985) ("[A] wiretap order which does not specify every person whose conversations may be intercepted does not *per se* amount to a 'virtual general warrant' in violation of the fourth amendment."); *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973) (holding that once the relevant authority for the search has been established as to one participant, the statements of other, incidental "participants may be intercepted if pertinent to the investigation").

215. *See* *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) ("To be sure, in the course of such wiretapping conversations of alien officials and agents, and perhaps of American citizens, will be overheard and to that extent, their privacy infringed. But the Fourth Amendment proscribes only 'unreasonable' searches and seizures."); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").

216. *In re Directives*, 551 F.3d at 1015.

217. *Id.*

218. *Id.*

219. *Id.* FISA's definition of minimization procedures, incorporated by the Protect America Act, includes procedures that require that non-publicly available information that is not foreign intelligence information "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

communications are incidentally acquired support the Fourth Amendment reasonableness of the surveillance.²²⁰ “On these facts, incidentally collected communications of non-targeted U.S. persons do not violate the Fourth Amendment.”²²¹

In conclusion, the Court of Review held that the procedures employed by the government were consistent with the considerations of *In re Sealed Case*.²²² Collectively, they required a showing of particularity, a “meaningful probable cause determination,” a showing of necessity, and a reasonable durational limit.²²³ The risks of error and abuse—which underlay many of the provider’s arguments—were “within acceptable limits and effective minimizations procedures [were] in place.”²²⁴ The court held that, balancing the vital nature of the government’s national security interest and the manner of the intrusion, “the surveillances at issue satisfy the Fourth Amendment’s reasonableness requirement.”²²⁵

V. Conclusion

The Court of Review’s decision in many ways spoke to the issues raised in the debate on the Protect America Act. On the one hand, it recognized the dangers of “indiscriminate executive power” and acknowledged that the “government cannot unilaterally sacrifice constitutional rights on the altar of national security.”²²⁶ Government surveillance for purposes of national security was bound by the Fourth Amendment.²²⁷ On the other hand, the court recognized that the government’s interest in the safety and security of its people was of “utmost significance.”²²⁸ The Court of Review’s role was to

foreign intelligence information or assess its importance.” Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(h)(2) (2006)).

220. The use of minimization procedures was cited by the Court of Review in its 2002 opinion as an important factor in ensuring the reasonableness of government surveillance under the Fourth Amendment. *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (citing *Scott v. United States*, 436 U.S. 128, 140–43 (1978)).

221. *In re Directives*, 551 F.3d at 1015.

222. *Id.* at 1016.

223. *Id.*

224. *Id.*

225. *Id.* The Court of Review described in summary form an argument—a “parting shot”—made by the provider for the first time at oral argument regarding “a specific privacy concern that could possibly arise under the directives.” *Id.* at 1015. The court held that, even assuming the provider had not waived this argument, “no issue falling within this description has arisen to date.” *Id.* at 1015. The court directed the government to notify the provider should the issue arise under the directives, but noted that there were safeguards in place that may satisfy the Fourth Amendment’s reasonableness requirement. *Id.* A more detailed discussion of the argument, safeguards, and the court’s holding is provided in the classified version of the court’s opinion. *Id.*

226. *Id.* at 1016.

227. *Id.*

228. *Id.*

balance those considerations.²²⁹ In this case, “where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions,” the court would not, in its own words, frustrate the government’s efforts to protect national security.²³⁰

The FISA Amendments Act of 2008 that followed the Protect America Act incorporates many of the statutory provisions and procedures that the Court of Review found important to its holding that the government’s surveillance was constitutional.²³¹ In particular, the FISA Amendments Act goes beyond the Protect America Act and imposes, for the first time, the requirement for a judicial finding that a U.S. person outside the United States targeted for surveillance or search is a “foreign power, an agent of a foreign power, or an officer or employee of a foreign power.”²³² This finding is made by the FISC under the FISA Amendments Act; as noted above, this finding was made previously by the Attorney General.²³³ In addition, the FISA Amendments Act expressly bans the “reverse targeting” of U.S. persons²³⁴ and requires FISC approval of the government’s targeting and minimization procedures.²³⁵ Incorporating many of the additional mechanisms the Court of Review relied upon in *In re Directives*, as well as many of the failings critics of the Protect America Act found in that statute, the FISA Amendments Act places on even firmer legal ground the execution of certain Fourth Amendment searches that are permitted by Congress and authorized and implemented by the Executive Branch without prior judicial review.

229. *See id.* (discussing the court’s role in balancing the need to protect individuals from unwarranted intrusions against the nature of the “government’s national security interest and the manner of the intrusion”).

230. *Id.*

231. Amnesty International, among others, has challenged the FISA Amendments Act as unconstitutional. *Amnesty Int’l USA v. McConnell*, 646 F. Supp. 2d 633, 634 (S.D.N.Y. 2009). In August 2009, the district court dismissed this facial challenge for lack of standing, and the appeal is still pending at the time of publication. *Id.* at 658.

232. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2449 (to be codified at 50 U.S.C. § 1881c(b)(3)(B)).

233. *See supra* notes 60, 190-194 and accompanying text.

234. FISA Amendments Act § 702.

235. *Id.*