RECENT DEVELOPMENTS

PROTECT AMERICA ACT OF 2007

On August 5, 2007, President Bush signed the Protect America Act of 2007 ("PAA") into law.[1] The Act was rushed through Congress at the behest of the Bush administration without any public hearings in either chamber.[2] Among other things, the PAA significantly changed the definition of "electronic surveillance" under the Foreign Intelligence Surveillance Act ("FISA") to exclude "surveillance directed at a person reasonably believed to be located outside the United States."[3] This change stripped the Foreign Intelligence Surveillance Court ("FISA Court") of jurisdiction to authorize such surveillance through prior orders known as "FISA warrants."[4] Instead, the PAA gave the Attorney General and the Director of National Intelligence the power to authorize telecommunication companies to acquire "foreign intelligence information concerning persons reasonably believed to be outside the United States" for periods of up to one year.[5] The Act also included a six-month sunset provision, which set the expiration date at February 1, 2008.[6]

Civil liberties groups, such as the American Civil Liberties Union and the Center for Democracy and Technology, were quick to criticize the PAA, claiming that it gave the government unconstitutionally broad powers to spy on Americans who have no involvement in terrorist activity.[7] Meanwhile, the Bush administration sought legislation that would give the Executive Branch greater flexibility to conduct surveillance, provide retroactive immunity for the private communications service providers that had provided electronic surveillance assistance to the government prior to passage of the PAA, and decline to set an expiration date.[8] By February 1, 2008, the PAA's

---

[1] Pub. L. No. 110-55, 121 Stat. 552 (2007) (amending the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1811 (2006)).

[2] *See* Charlie Savage, *New Law Expands Power to Wiretap*, BOSTON GLOBE, Aug. 6, 2007, at A1; *see also* Joby Warrick & Walter Pincus, *How the Fight for Vast New Spying Powers Was Won*, WASH. POST, Aug. 12, 2007, at A1.

[3] Protect America Act, sec. 2, § 105A, 121 Stat. 552, 552 (2007).

[4] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1804–1805 (2006) (prior to PAA amendments); *see also* Greg Miller, *Spy Chief Sheds Light on Wiretaps*, L.A. TIMES, Aug. 23, 2007, at A14.

[5] Protect America Act, sec. 2, § 105B, 121 Stat. 552, 552 (2007).

[6] Protect America Act, Pub. L. No. 110-55, § 6, 121 Stat. 552, 556 (2007).

[7] *See, e.g.*, American Civil Liberties Union, Fact Sheet on the "Police America Act," Aug. 7, 2007, http://www.aclu.org/safefree/nsaspying/31203res20070807.html; Press Release, Ctr. for Democracy and Tech., Congress Votes to Expand Unchecked Warrantless Wiretapping (Aug. 5, 2007), *available at* http://www.cdt.org/press/20070805press.php.

[8] *See* Press Release, The White House, FISA 101: Why FISA Modernization Amendments Must Be Made Permanent (Sept. 19, 2007), *available at* http://www.whitehouse.gov/news/releases/2007/09/20070919-1.html.

original expiration date, Congress had not found a permanent solution. Instead, it extended the PAA until February 15.[9]

This Recent Development analyzes the PAA's most important provisions, examines the circumstances surrounding its passage, summarizes criticisms and potential legal challenges to the PAA, and evaluates some proposed bills pending in Congress to make long-term changes to FISA. It argues that any long-term statutory scheme that Congress enacts must contain oversight and reporting provisions that make information available about the degree to which Americans are relinquishing their privacy rights in the name of national security. If the government makes the details of its electronic surveillance program readily available, the American people will be able to hold a better informed public debate on the appropriate balance between privacy and security. This Recent Development also argues that granting retroactive immunity to the communications service providers that assisted the government prior to the passage of the PAA should not be part of a long-term solution. If in fact these companies did cooperate with unlawful government mandates, holding them accountable will encourage them to scrutinize the legality of similar mandates in the future. Instead, given that private companies are entrusted with protecting their customers' privacy but have little incentive to do so under the PAA, Congress should consider providing additional incentives for private companies to challenge unlawful government directives for surveillance assistance.

I. How the PAA Changed FISA

A. Definition of Electronic Surveillance

Prior to the passage of the PAA, "surveillance directed at a person reasonably believed to be located outside the United States" fell under the four-part definition of "electronic surveillance" in section 104 of FISA. The PAA changed the definition of "electronic surveillance," stating that "nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States."[10] By redefining "electronic surveillance," the PAA moved a significant set of intelligence activity outside FISA's regulatory scheme.

FISA formerly defined "electronic surveillance" as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the United

[9] Pub. L. No. 110-182, 122 Stat. 605 (2008) (passed by voice vote in both houses as H.R. 5104 on Jan. 29, 2008).

[10] *Compare* Protect America Act, sec. 2, § 105A, 121 Stat. 552, 552 (2007), *with* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(f) (2006).

States . . . ."[11] Under the PAA, however, if the government wiretapped a communication between a person reasonably believed to be located outside the U.S. and a person in the U.S., and the purpose of the government's surveillance was to gather information about the person abroad, that surveillance would not be "electronic surveillance."

Similarly, prior to the passage of the PAA, section 101(f)(4) of FISA defined "electronic surveillance" as "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[12] Again, under the PAA, if the government intercepted a communication between a person reasonably believed to be abroad and a person in the U.S. and the purpose of the government's surveillance was to gather information about the person abroad, that surveillance would not be "electronic surveillance" under the amended FISA.

By changing the definition of "electronic surveillance," the PAA removed conduct that would have met the definition of electronic surveillance under the previous version of FISA from the jurisdiction of the FISA Court. The FISA Court has the authority "to hear applications for and grant orders approving electronic surveillance anywhere within the United States."[13] Because the PAA removed activity that gathers information about individuals abroad from the definition of "electronic surveillance," the FISA Court no longer had jurisdiction to issue warrants that pre-approved plans for such activity.[14]

B. New Procedures for Acquiring Foreign Intelligence

The PAA shifted the power to authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" from the FISA Court to the Director of National Intelligence ("DNI") and the Attorney General ("AG").[15] To exercise this power, both the DNI and the AG had to certify that: (1) there were "reasonable procedures in place for determining that the acquisition . . . concerns persons reasonably believed to be located outside the United States . . . ."; (2) the acquisition did not constitute electronic surveillance; (3) the acquisition involved obtaining the information from or with the assistance of a communications service provider who had access to communications either as they were transmitted or while they were stored; (4) a significant purpose of the

[11] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(f)(2) (2006) (prior to PAA amendments).

[12] *Id.* § 1801(f)(4) (prior to PAA amendments).

[13] *Id.* § 1803(a).

[14] *See id.*

[15] Protect America Act, sec. 2, § 105B(a), 121 Stat. 552, 552 (2007).

acquisition was to obtain foreign intelligence information; and (5) "minimization procedures"[16] were used to minimize the privacy impact to U.S. persons.[17] However, the certification did not require particularity; the DNI and the AG did not need to identify the specific facilities, places, premises, or properties that would be the targets of efforts to acquire intelligence.[18]

In "emergency situations," the PAA allowed the DNI and the AG to make their required certifications up to seventy-two hours after the acquisition of foreign intelligence.[19]

C. Cooperation with the Private Sector

The PAA allowed the government to direct private companies and their employees to assist in gathering intelligence, compensate them for their participation, invoke the courts' assistance in compelling compliance with the initial directive, and threaten them with contempt of court if they refused.[20] It also allowed private companies to challenge those orders in court and immunized cooperating companies from private suits.[21]

D. Court Review

The PAA provided a limited role for judicial supervision of the government's intelligence activities. The procedures used by the DNI and the AG in determining that the government's foreign intelligence activities actually concerned persons reasonably believed to be located outside the U.S. was "subject to review of the [FISA Court] pursuant to section 105C."[22] Additionally, the FISA Court had the authority to review the procedures "by which the [g]overnment determines that acquisitions conducted . . . [did] not constitute electronic surveillance," albeit under the deferential "clearly erroneous" standard.[23] The government could petition the Supreme Court to appeal a FISA Court determination.[24] However, the DNI and the AG were neither required nor permitted to seek the approval of any court before au-

[16] 50 U.S.C. § 1801(h) (prior to PAA Amendments).

[17] Protect America Act, sec. 2, § 105B(a), 121 Stat. 552, 552 (2007). In section 1801(i), FISA defines a U.S. person as a "citizen of the United States, an alien lawfully admitted for permanent residence . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States . . . ." 50 U.S.C. §1801(i).

[18] Protect America Act, sec. 2, § 105B(b), 121 Stat. 552, 552 (2007).

[19] *Id.* sec. 2, § 105B(a), 121 Stat. 552, 552 (2007). FISA does not define "emergency situation." *See* Foreign Intelligence Surveillance Act, 50 U.S.C.A. §§ 1801–1811. (West 2007).

[20] *See* Protect America Act, sec. 2, § 105B(e)–(i), 121 Stat. 552, 553–54 (2007).

[21] *Id.* sec. 2, § 105B(h)–(l), 121 Stat. at 554.

[22] *Id.* sec. 2, § 105B(a)(1), 121 Stat. at 552.

[23] *Id.* sec. 2, § 105C(b), 121 Stat at 555.

[24] *Id.* sec. 2, § 105B(d), 121 Stat. at 553.

thorizing intelligence gathering "directed at a person reasonably to be located outside the United States."[25]

E. Records and Reporting

The PAA also had a reporting component, although its scope was limited. Certifications by the DNI and the AG that approved the intelligence gathering procedures had to be transmitted to the FISA Court under seal.[26] The PAA required the DNI and the AG to report to Congress regarding their compliance with the certification requirement.[27] These offices were also obligated to provide information to the Intelligence and Judiciary Committees in both the House and the Senate about the acquisitions made during the previous six month period.[28] These reports had to describe all failures of intelligence officers to comply with relevant guidelines and procedures and all incidents of communications service providers refusing to comply with directives requiring participation in intelligence gathering activities.[29] The reports also had to include the number of certifications and directives the DNI and the AG issued during the reporting period.[30] Notably, however, the PAA did not require the DNI and the AG to disclose how many Americans abroad they targeted or how many conversations between Americans within the U.S. and persons reasonably believed to be abroad they intercepted.

F. Sunset and Transition

The PAA was set to expire on February 1, 2008, 180 days after its enactment.[31] At that time, any existing authorizations were to remain in effect until they expired.[32]

II. The Legislative History of the PAA

Congress originally passed FISA in response to revelations that the government misused its ability to gather electronic surveillance for national security purposes during the Cold War.[33] To address this problem, Congress

---

[25] *Id.* sec. 2, § 105B(b)–(d), 121 Stat. at 553.

[26] *Id.* sec. 2, § 105B(c), 121 Stat. at 553.

[27] *Id.* sec. 2, § 105B(d), 121 Stat. at 553. Such procedures could include the minimization procedures or the procedures for determining that the acquisition of foreign intelligence concerns persons reasonably believed to be outside the U.S. *See* Elizabeth B. Bazan, Cong. Research Serv., The Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act 8 (2007).

[28] Protect America Act, Pub. L. No. 110-55, § 4, 121 Stat. 552, 555 (2007).

[29] *Id.*

[30] *Id.*

[31] *Id.* § 6, 121 Stat. at 556.

[32] *Id.*

[33] *See* S. Rep. No. 94-755, at 12 (1976) (Book II, Church Committee Report); *see also* H.R. Rep. No. 110-373, pt. 2, at 11–12 (2007) (summarizing FISA's legislative history, and

sought to strike a balance between national security interests and civil liberties.[34] The legislative history of FISA is replete with concerns about the effect of electronic surveillance on privacy rights under the Fourth Amendment and the chilling effect surveillance could have on activities protected by the First Amendment.[35] FISA has been amended several times since 1978[36] and a few times since the terrorist attacks of September 11, 2001.[37]

After September 11, 2001, the Bush administration launched the secret Terrorist Surveillance Program ("TSP") outside of the FISA statutory framework.[38] The TSP allowed "intercepts of contents of communications where one . . . party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[39] The press revealed the existence of the program in December 2005.[40]

The Bush administration based its legal authority to conduct the TSP on the Congressional Authorization for the Use of Military Force.[41] In January 2007, a FISA judge reportedly issued orders which brought the TSP under

noting that "in the 1960s, NSA began adding to its 'watch lists,' at the request of various intelligence agencies, the names of American suspected of involvement in civil disturbance or drug activity which had some foreign aspects. Second, Operation Shamrock, which began as an effort to acquire the telegrams of certain foreign targets, expanded so that NSA obtained from at least two cable companies essentially all cables to or from the United States, including millions of the private communications of Americans.") (internal citations omitted).

[34] *See* H.R. REP. NO. 110-373, pt.2, at 12 (2007).

[35] *See id.* at 11–12.

[36] *See* Pub. L. No. 95-511, tit. I, § 105, 92 Stat. 1790 (1978); Pub. L. No. 98-549, § 6(b)(3), 98 Stat. 2804 (1984); Pub. L. No. 106-567, tit. VI, § 602(b), 114 Stat. 2851(2000).

[37] *See* Pub. L. No. 107-56, tit. II, §§ 206, 207(a)(1), (b)(1), 225, 115 Stat. 282, 295 (2001); Pub. L. No. 107-108, tit. III, § 314(a)(2), (c)(1), 115 Stat. 1402, 1403 (2001); Pub. L. No. 107-273, div. B, tit. V, § 4005(c), 116 Stat. 1812 (2002); Pub. L. No. 108-458, title I, § 1071(e), 118 Stat. 3691 (2004); Pub. L. No. 109-177, tit. I, §§ 105(a), 108(a)(2), (b), 120 Stat. 195, 203 (2006).

[38] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, A22; *see also* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 565 (2007).

[39] *See* Press Release, The White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005).

[40] *See* Risen & Lichtblau, *supra* note 38. R

[41] Letter from U.S. Dep't of Justice to Sen. Harry Reid (R-Nev.), Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *available at* http://www.usdoj.gov/ag/readingroom/surveillance9.pdf (citing Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (2001) (reported as a note to 50 U.S.C.A. § 1541 (2001))); *see also* Yoo, *supra* note 38, at 586 (arguing that the TSP represents a valid exercise of the President's Commander-in-Chief authority to gather intelligence during wartime). R

the control of the FISA court, an action the Bush administration perceived as a hindrance to its surveillance activities.[42]

Although it abandoned the TSP, the Bush administration continued to prioritize national security. In July 2007, the National Intelligence Council released an unclassified summary of the National Intelligence Estimate on The Terrorist Threat to the U.S. Homeland which showed a continuing threat of terrorist attack.[43] The DNI, Admiral Mike McConnell, proposed changes in FISA to meet the current intelligence needs of the nation.[44] Specifically, Admiral McConnell argued that gathering intelligence from foreign targets located overseas should not require a prior court order, and he asked for liability protection for communications service providers and their employees who had assisted the government in carrying out its foreign intelligence collection efforts under the TSP.[45] Agreeing with Admiral McConnell's position, on April 12, 2007, the Bush administration announced that it had submitted draft legislation that would amend FISA to include a program like the TSP.[46]

On August 1, 2007, just days before Congress was scheduled to go on recess, Senator Mitch McConnell (R-Ky.) introduced the PAA, a bill that satisfied most of the Bush administration's requests. Pressuring Congress to pass the bill quickly, President Bush stated that he opposed Congress's adjournment for its summer recess unless it approved "a bill I can sign."[47] The bill passed in the Senate on August 3 by a vote of 60 to 28.[48] The House took up the bill on August 4 and passed it the same day by a vote of 227 to 183.[49]

---

[42] Carol D. Leonnig & Ellen Nakashima, *Ruling Limited Spying Efforts*, WASH. POST, Aug. 3, 2007, at A1 (stating that the judge's decision effectively curtailed necessary surveillance and too limited the flow of information about possible terrorism suspects). *But see* Interview by Chris Roberts with Mike McConnell, DNI, in El Paso, Tex., *available at* http://www.elpasotimes.com/news/ci_6685679 (last visited Apr. 3, 2008)(suggesting that it was a FISA Court ruling on May 31, 2007, that slowed spying efforts: "After the 31st of May we were in extremis because now we have significantly less capability."); *see also* Warrick & Pincus, *supra* note 2, at A1 (stating that in May 2007 a judge told the administration flatly that FISA's wording required the government to get a warrant whenever a fixed wire was involved). **R**

[43] NAT'L INTELLIGENCE COUNCIL, NATIONAL INTELLIGENCE ESTIMATE ON THE TERRORIST THREAT TO THE US HOMELAND 6–7 (2007) *available at* http://www.odni.gov/press_releases/20070717_release.pdf.

[44] Press Release, Office of the Dir. Of Nat'l Intelligence, Modernization of the Foreign Intelligence Surveillance Act (FISA) (Aug. 2, 2007), *available at* http://www.odni.gov/press_releases/20070802_release.pdf (last visited Apr. 3, 2008).

[45] *See id.*

[46] *See* S. REP. NO. 110-209, at 5 (2007).

[47] Joby Warrick & Ellen Nakashima, *Senate Votes to Expand Warrantless Surveillance; White House Applauds; Changes are Temporary*, WASH. POST., Aug. 4, 2007, at A1.

[48] 153 CONG. REC. S10,871 (daily ed. Aug. 3, 2007).

[49] 153 CONG. REC. H9,965 (daily ed. Aug. 4, 2007).

III. The Policy Debate

A. Critics of the PAA

Civil liberties groups (such as the American Civil Liberties Union ("ACLU") and the Center for Technology and Democracy ("CDT")), academics, and others sharply criticized the PAA.[50] Critics made constitutional and policy arguments against the PAA and suggested several changes to be incorporated in any permanent statutory scheme governing electronic surveillance.

Some criticized the PAA on Fourth Amendment grounds. For example, Peter Dempsey, Policy Directory for CDT, argued that the PAA authorized unconstitutional searches of Americans when searches that targeted individuals outside the U.S. incidentally collected information on Americans.[51] Dempsey also argued that such searches violate the Fourth Amendment because they are not based on probable cause and are not reasonably limited in duration.[52] Similarly, the ACLU claimed that U.S. persons were no longer protected from warrantless surveillance under the PAA, and called the PAA an "unconstitutional program warrant that doesn't state with specificity the things to be searched or seized."[53]

Others charged that the PAA should require stronger Congressional and Judicial oversight of surveillance programs, in light of the fact that the TSP was operational for over five years in complete secrecy.[54] For example, Professor John Sims of the University of California wrote: "given the illegality of the warrantless surveillance program and the tenacity with which the [Bush] Administration has clung to its sweeping claim of Article II authority to violate FISA at will, Congress and the public must subject any pro-

---

[50] *See* American Civil Liberties Unions, *supra* note 7; Press Release, Ctr. For Democracy & Tech., *supra* note 7; *FISA for the Future: Balancing Security and Liberty: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. (2007) [hereinafter *FISA for the Future*] (statement of James X. Dempsey, Policy Dir., Ctr. for Democracy & Tech.); *see also Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security: Hearing before the S. Comm. on the Judiciary*, 110th Cong. (2007) [hereinafter *Strengthening FISA*] (statement of Suzanne E. Spaulding, Principal Bingham Consulting LLC, Of Counsel, Bingham McCutchen LLP). R

[51] *See FISA for the Future* (statement of James X. Dempsey), *supra* note 50; *see also* Mayfield v. U.S., 504 F. Supp. 2d 1023 (D. Or. 2007) (holding that Patriot Act provisions authorizing surveillance and searches pursuant to FISA if "a significant purpose" of the surveillance was the gathering of foreign intelligence violated Fourth Amendment by permitting the Executive Branch to conduct surveillance and searches of American citizens without first proving to an objective and neutral magistrate that probable cause existed to believe a crime had been committed). R

[52] *See FISA for the Future*, *supra* note 50 (statement of James X. Dempsey). R

[53] ACLU Analysis of the Protect America Act, Aug. 29, 2007, http://www.aclu.org/safefree/general/31496leg20070829.html.

[54] *See, e.g.*, John Cary Sims, *How the Bush Administration's Warrantless Surveillance Program Took the Constitution on an Illegal, Unnecessary, and Unrepentant Joyride*, 12 UCLA J. Int'l L. & Foreign Aff. 163 (2007) (arguing that the TSP was unconstitutional on separation of powers grounds).

posed FISA amendments to an informed and skeptical analysis."[55] Similarly, Suzanne E. Spaulding, former Assistant General Counsel at the CIA, criticized the fact that the minimization requirements for acquisitions authorized by the DNI and the AG were internal policies that the Executive Branch could change unilaterally, avoiding checks by the Legislative and Judicial Branches.[56] She also advocated for a robust role for the FISA Court judges, citing the "Keith Case" for the proposition that "unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[57] The ACLU also contended that the PAA gives too much leeway to the intelligence community in general, and the National Security Agency ("NSA") in particular, given their long histories of abusing their authority whenever their exercise of power is not carefully monitored.[58] The Center for Security Studies recommended requiring periodic reports to Congress detailing how many communications by Americans are intercepted, analyzed, or retained by the government.[59]

Critics also pointed out that the PAA authorized far broader warrantless surveillance than the TSP did.[60] The TSP only authorized warrantless surveillance of Americans communicating with al Qaeda and associates, whereas the scope of the PAA is potentially much broader.[61]

Other critics suggested that as a policy matter, the PAA may not have been necessary. According to James Baker, former Counsel for Intelligence Policy at the Department of Justice, the original FISA contributed significantly to U.S. successes against al Qaeda and other terrorist groups post-9/11, and FISA even worked during wartime.[62] Others argued that the PAA potentially makes the U.S. less safe. For example, Susan Landau claimed that the new PAA creates a security risk by building massive automatic sur-

---

[55] *Id.* at 166.

[56] *Strengthening FISA*, *supra* note 50 (statement of Suzanne E. Spaulding). R

[57] *Id.* (citing United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 317 (1972); *see also* Warrick & Nakashima, *supra* note 47 (stating that Democrats in the House failed to win support for more modest changes that would have required closer court supervision of government surveillance). R

[58] *See* Letter from Caroline Fredrickson, Dir., Wash. Legislative Office, to Rep. John Dingell (D-Mich.), Chairman of Comm. on Energy and Commerce (Oct. 12, 2007); s*ee also* American Civil Liberties Union, *supra* note 7; Eric Lichtblau, *F.B.I. Gained Unauthorized Access to E-Mail*, N.Y. TIMES, Feb. 17, 2008, at A1. R

[59] *See FISA for the Future*, *supra* note 50 (statement of Lisa Graves, Deputy Dir., Ctr. for Nat'l Sec. Studies). R

[60] *See* Warrick & Nakashima, *supra* note 47. R

[61] The PAA is not limited to information pertaining to terrorism or national security, and the ambiguity of the language of "acquisition," "information," and "concerning," in section 105B of the PAA may leave a substantial amount of surveillance activity outside of the control of the FISA Court.

[62] *See FISA for the Future*, *supra* note 50 (statement of James Baker, Lecturer on Law, Harvard Law Sch.) (pointing to the success under the pre-PAA FISA); *see generally* James A. Baker, *Intelligence Oversight*, 45 HARV. J. ON LEGIS. 199 (2008). R

veillance capabilities into telephone switches that could be intercepted by enemies.[63]

B. Supporters of the PAA

Members of the intelligence community generally supported the PAA and advocated for further changes to FISA. The DNI, Admiral McConnell, testified before the House Intelligence Committee on September 20, 2007, and reiterated his support for the PAA and making its amendments to FISA permanent.[64] To assuage civil liberties groups' fears that the government would be conducting warantless surveillance on Americans overseas, McConnell cited section 2.5 of Executive Order 12333, which requires that the AG make an individualized finding that there is probable cause to believe than an American abroad is an agent of a foreign power before the government may gather intelligence or conduct a physical search of that person.[65] He also pointed to the PAA's minimization procedures and emphasized that targeting Americans in the U.S. is unlawful.[66] Furthermore, he stated that detecting sleeper cells within the U.S. was an important factor in favor of maintaining the PAA's exemption to the definition of electronic surveillance.[67]

McConnell also suggested that the PAA might not have gone far enough in modernizing FISA.[68] He called for the changes effected by the PAA to be made permanent and urged that the FISA process be further streamlined by simplifying the application for FISA court orders, increasing the number of senior Executive Branch national security officials who can authorize FISA certifications, increasing the period of time for which the FISA Court could authorize surveillance, and extending the emergency authorization period beyond the seventy-two hours currently permitted.[69] Furthermore, he called for Congress to provide liability protection for the private companies that participated in the TSP.[70]

Kenneth Wainstein, Assistant AG for National Security at the Department of Justice, also testified before Congress in support of the PAA.[71] He pointed out that considerable resources of the Executive Branch and the

---

[63] Susan Landau, Editorial, *A Gateway for Hackers: The Security Threat in the New Wiretapping Law*, WASH. POST, Aug. 9, 2007, at A17.

[64] *Full Committee Hearing—Administration Views of FISA Authorities: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. (2007) (statement of Adm. Mike McConnell, DNI) [hereinafter *FISA Authorities Hearing*].

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *See id.*

[69] *See id.*

[70] *Id.*; *see also* Mike McConnell, Letter to the Editor, *Help Me Spy on Al Qaeda,* N.Y. TIMES, Dec. 10, 2007, at A23.

[71] *FISA Authorities Hearing*, supra note 64 (statement of Kenneth Wainstein, Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice).

FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad and that a simpler process might be less costly.[72] He emphasized that the PAA did not authorize the physical search of homes, personal effects, computers, or mail of individuals within the United States, and that "to the extent that [section 105B] could be read to authorize the collection of business records of individuals in the United States on the theory that they 'concern' persons outside the United States, we wish to make very clear that we will not use this provision to do so."[73] Bryan Cunningham, Former CIA Assistant General Counsel, pointed out that the U.S. government has conducted surveillance on communications between non-U.S. persons constitutionally for decades (in contexts not governed by FISA), despite the possibility that the government would inadvertently be intercepting the communications of U.S. persons without a warrant.[74] According to Cunningham, because the government has stayed within the bounds of the Constitution in conducting past surveillance activities, critics' fears about government abuse of the PAA's breadth may be overblown.[75]

IV. Unresolved Legal Issues

A. The Scope of the Fourth Amendment in Surveillance

The extent to which the Fourth Amendment constrains Congress's ability to authorize the gathering of intelligence is unsettled. The Fourth Amendment protects U.S. citizens from warrantless surveillance inside the United States.[76] The Fourth Amendment also proscribes domestic surveillance of lawful resident aliens.[77] However, the Supreme Court has not taken a clear stance on the scope of the Fourth Amendment's protection in the context of foreign intelligence surveillance, and the U.S. Circuit Courts of Appeal are

[72] *Id.*

[73] *Id.*

[74] *Hearing Before the S. Comm. on the Judiciary*, 110th Cong. (2007) (statement of Bryan Cunningham, Principal, Morgan & Cunningham LLC) (citing United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) for the proposition that the President has inherent constitutional authority to approve warrantless wiretaps for foreign intelligence purposes). For analysis of Fourth Amendment doctrine regarding surveillance powers, see Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 74 U. Chi. L. Rev. (forthcoming 2008), *available at* http://ssrn.com/abstract=1000398.

[75] *See id.*

[76] *See* Katz v. United States, 389 U.S. 347, 353, 359 n.23 (1967); *see also* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313–14, 320–21 (1972) (requiring a warrant for domestic electronic surveillance, but reserving judgment on whether a warrant would be required for foreign surveillance).

[77] See United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (suggesting that the Fourth Amendment applies to aliens who have accepted societal obligations and made a significant voluntary commitment to the U.S.).

split on the issue.[78] One federal district court recently held that some of the warrantless surveillance provisions of FISA, as amended by the Patriot Act, are unconstitutional.[79]

B. Cases Concerning Private Participation in the TSP and Potential Retroactive Immunity

There are over fifty lawsuits[80] pending in which the parties charge that the TSP was unconstitutional and violated FISA.[81] Many of those have been consolidated before the U.S. District Court in San Francisco.[82] Plaintiffs litigating these claims have struggled against two legal doctrines to win damages for their injuries under the TSP. First, plaintiffs often cannot establish standing to bring their claims because they cannot demonstrate a personal injury caused by communications service providers' participation in the TSP.[83] Second, the government has used the state secrets doctrine, "a common law evidentiary privilege that permits the government to bar the disclosure of information if 'there is a reasonable danger' that disclosure will 'expose military matters which, in the interest of national security, should

[78] *See, e.g.,* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) (holding that warrantless electronic surveillance is lawful if its primary purpose is to gather foreign intelligence information, but stating that "government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborator."); United States v. Buck, 548 F.2d 871 (9th Cir. 1977) (holding that foreign security wiretaps are a recognized exception to the general warrant requirement); Zweibon v. Mitchell, 516 F.2d 594, 613–14 (D.C. Cir. 1975) (holding that warrants are required to wiretap domestic organizations); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) (en banc) (holding that a warrant is not required when surveillance is directed at non-U.S. persons, but stating that "the foundation of any determination of reasonableness . . . is the probable cause standard."); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence).

[79] Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007). *But see* United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 303, 313 (D. Conn. 2008) (holding that FISA, as amended by the Patriot Act does not violate the Fourth Amendment on its face or as applied); United States v. Mubayyid, 521 F. Supp. 2d 125, 136 (D. Mass. 2007); *In re* Sealed Case No 02-001, 310 F.3d 717 (FISA Ct. Rev. 2003) (concluding that FISA as amended by the Patriot Act is constitutional because the surveillances it authorizes are "reasonable" under the Fourth Amendment).

[80] *See*, *e.g.,* Hepting v. AT&T, 439 F. Supp. 2d. 974, 984 (N.D. Cal. 2006); Al Haramain Islamic Found. v. Bush, 507 F.3d 1190 (9th Cir. 2007); ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated and remanded on other grounds*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 128 S.Ct. 1334 (2008) (the district court held the plaintiffs' data-mining claim was barred by the state secrets privilege). The Sixth Circuit recently held that a group of plaintiffs, who could not show that they personally were injured by TSP because the state secrets doctrine prevented them from obtaining proof that they were among the group surveilled under the program, lacked standing to challenge the TSP. 493 F.3d at 644.

[81] *See* Karl Vick, *Judges Skeptical of State-Secrets Claim*, WASH. POST, Aug. 16, 2007, at A4.

[82] *In re* NSA, Telecomm. Records Litig., 2007 U.S. Dist. LEXIS 53456 (N.D. Cal. 2007).

[83] *See* Recent Case*, Sixth Circuit Denies Standing to Challenge Terrorist Surveillance Program*, 121 HARV. L. REV. 922 (2008) (arguing that standing rules should be relaxed).

not be divulged," to prevent plaintiffs from pursuing claims under the TSP.[84] In *Al Haramain Islamic Foundation v. Bush*, the government asserted that litigation concerning injuries allegedly caused by the TSP should be dismissed because it would necessarily reveal state secrets.[85] Nevertheless, the Bush administration wants any permanent amendment of FISA to provide retroactive immunity to protect private companies that helped the government conduct the TSP against the threat of liability.[86]

Congressional discussions about permanent legislation amending FISA have focused on four strategies to limit private companies' liability: blanket immunity, targeted immunity, substitution, and indemnification.[87] As the name suggests, blanket immunity would immunize everyone with any connection to the program, including government officials.[88] Targeted immunity would only cover companies that could prove they were participating in the TSP in good faith.[89] Substitution takes a different approach, substituting the government for the private company as the defendant in the litigation.[90] Finally, the indemnification strategy allows cases against communications service providers to proceed through the court system with the understanding that the government would assume any damages.[91]

Proponents of retroactive immunity in the Senate[92] argue that the companies participating in the TSP should not be liable because they relied in good faith on government assurances that the TSP directives were lawful.[93] They also contend that if companies are subject to liability they will be deterred from assisting in the future,[94] which is harmful because the cooperation of private companies is an indispensable part of a successful electronic surveillance program.[95] Finally, they fear that classified information will be made public during legal proceedings.[96]

---

[84] *Al Haramain Islamic Found.*, 507 F.3d at 1205 ("Al-Haramain cannot establish that it suffered injury in fact, a 'concrete and particularized' injury, because the Sealed Document, which Al-Haramain alleges proves that its members were unlawfully surveilled, is protected by the state secrets privilege.").

[85] *See id.*

[86] *See* S. REP. NO. 110-209, at 7 (2007).

[87] Ellen Nakashima, *Democrats to Offer New Surveillance Rules; Bill Aims to Meet Privacy and Security Concerns; Fierce Debate is Expected,* WASH. POST, Oct. 7, 2007, at A4.

[88] *See id.*

[89] *See id.*

[90] *See id.*

[91] *See id.*

[92] *See*, *e.g.*, S. REP. NO. 110-258, at 35 (2007) (minority views of Sen. Jon Kyl (R-Ariz.), Sen. Orrin Hatch (R-Utah), Sen. Chuck Grassley (R-Iowa), Sen. Jeff Sessions (R-Ala.), Sen. Lindsey Graham (R-S.C.), Sen. Tom Coburn (R-Okla.), and Sen. Sam Brownback (R-Kan.)).

[93] *See* S. REP. NO. 110-209, at 9 (2007) (determining that electronic communications service providers acted on a good faith belief that the President's program—and their assistance—was lawful).

[94] See S. REP. NO. 110-258, at 35 (2007).

[95] *Id.* at 10.

[96] *Id.*

Opponents of retroactive immunity in the Senate[97] argue that private suits may be the only way that plaintiffs can remedy injuries to their privacy caused by the TSP.[98] Some also argue that the Bush administration has not given Congress sufficient information about the TSP for it to determine whether immunity is appropriate.[99]

Congress should not grant immunity to these communications providers. Before the passage of the PAA, FISA contemplated civil liability for companies that assisted in surveillance that violated FISA's provisions, and private companies knew that they could only assist the government under FISA-compliant orders.[100] If permanent legislation amending FISA grants retroactive immunity, companies will suffer no adverse consequences for complying with government directives that unlawfully infringe on Americans' privacy. Granting retroactive immunity will provide a disincentive for companies to challenge unlawful directives in the future.[101] Combined with the financial incentive to comply with all directives,[102] a rational company would be unlikely to resist any directive, no matter how profoundly it might violate its customers' privacy.

If anything, Congress should increase rather than reduce incentives to challenge unlawful surveillance directives. One method of doing so is to have the government pay attorneys' fees to private companies that successfully challenge a directive. Congress has already created a similar incentive to challenge government actions under the Equal Access to Justice Act, which pays attorneys' fees to individuals and small businesses that successfully bring suit against the government.[103]

V. New Bills

After the PAA was passed, the House and the Senate separately considered legislation to make long-term amendments to FISA. The House considered the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007 ("The RESTORE Act"), H.R. 3773, while the Senate considered the FISA Amendments Act of 2007, S. 2248.[104] In the meantime, the PAA was set to expire on February 1, 2008. On January 29,

[97] *See, e.g.*, *id.* at 19 (additional views of Sen. Patrick Leahy (D-Vt.)) ("[B]lanket retroactive immunity . . . undermines accountability and the rule of law.").

[98] *See* Elizabeth B. Bazan, Cong. Research Serv., The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues 14-15 (2007).

[99] *Id.* at 15.

[100] S. Rep. No. 110-258, at 20 (2007) (additional views of Sen. Leahy).

[101] *Id.*

[102] *See supra* note 20 and accompanying text. R

[103] *See* 5 U.S.C. § 504 (2000); 28 U.S.C. § 2412 (2000).

[104] For a detailed, side-by-side comparison of the legislation being considered in both chambers, see Elizabeth B. Bazan, Cong. Research Serv., The Foreign Intelligence Surveillance Act: Comparison of House Passed H.R. 3773, S. 2248 as Reported by the Senate Select Committee on Intelligence, and S. 2248 as Reported Out of the Senate Judiciary Committee (2007).

the House and the Senate unanimously passed H.R. 5104, Public Law 110-182, extending the PAA until February 16, 2008.[105] On February 16, however, Congress had not agreed on legislation to make long-term amendments to FISA. This Section discusses the legislative proposals to amend FISA considered in the House and the Senate from fall of 2007 until March 15, 2008.

The House responded more quickly than the Senate in passing a potential long-term replacement to the PAA. On October 9, 2007, Representative John Conyers (D-Mich.) introduced the RESTORE Act, which was referred to the House Permanent Select Committee on Intelligence and the House Committee on the Judiciary.[106] Both Committees reported favorably on the bill as amended on October 12.[107] The bill passed in the House by a vote of 227 to 189 on November 15, 2007.[108]

The RESTORE Act differed starkly from the PAA and the proposals of the Bush Administration in several ways. First, it abandoned the PAA's limitation on the definition of electronic surveillance.[109] Instead, it provided that no court order was necessary for

> electronic surveillance directed at acquisition of contents of communications between persons not known to be United States persons and are reasonably believed to be located outside the United States . . . without respect to whether the communication passes through the United States or the surveillance device is located within the United States.[110]

Second, it created the concept of "basket orders," which allows the FISA Court to authorize surveillance of targets overseas as long as the FISA Court has approved the procedures for determining certain facts about the surveillance targets. To approve the procedures for gathering this information, the FISA Court must show that the targets are reasonably likely to be overseas. The Court must also identify the procedures for handling communications by Americans intercepted by those orders and the guidelines to be followed when the significant purpose of an acquisition is to acquire the communications of a specific United States person reasonably believed to be located in the United States.[111] The bill also required quarterly FISA Court review of

---

[105] Paul Kane, *Congress Passes 15-Day Extension of Surveillance Law*, WASH. POST, Jan. 30, 2008, at A4. The bill, H.R. 5104, passed by voice vote in the House and unanimous consent in the Senate. 154 CONG. REC. H517 (daily ed., Jan. 29, 2008),

[106] H.R. 3773, 110th Cong. (2008); 153 CONG. REC. E2088 (daily ed. Oct. 9, 2007) (statement of Rep. Conyers).

[107] *See* H.R. REP. NO. 110-373, pt. 1 (2007); *see also* H.R. REP. NO. 110-373, pt. 2 (2007).

[108] 153 CONG. REC. H14,062-61 (daily ed. Nov. 15, 2007) (roll call vote no. 1120).

[109] *See* BAZAN, *supra* note 104, at 3. R

[110] H.R. 3773, 110th Cong. § 2 (2007) (as passed by House).

[111] *Id.* § 3 (requiring that "a significant purpose of the acquisition [be] to obtain foreign intelligence information," and that the surveillance targets: (1) "are reasonably believed to be located outside the United States"; (2) "may be communicating with persons inside the United States"; and (3) "are reasonably believed to be persons that are not United States persons.");

these "basket orders" to assess the circumstances under which information concerning U.S. persons was acquired, retained, and disseminated.[112] Third, it authorized the DNI and the AG to authorize—for a forty-five-day period—the emergency acquisitions of communications of non-U.S. persons located outside the U.S. who may be communicating with persons inside the U.S.[113] Fourth, it provided for regular reporting to Congress on electronic surveillance,[114] and an audit of all warrantless surveillance that occurred after September 11, 2001, (including the TSP) by the Inspectors General of the Department of Justice, the Office of the DNI, and the National Security Agency ("Inspectors General").[115] Fifth, it provided that, "notwithstanding any other provision of law, [FISA] shall be the exclusive means by which electronic surveillance may be conducted for the purpose of gathering foreign intelligence information."[116] Finally, the RESTORE Act was set to expire on December 31, 2009.[117] Notably, the RESTORE Act did not grant retroactive immunity to communications service providers that assisted the government in electronic surveillance after September 11, 2007.[118]

In contrast, the FISA Amendments Act took several months to make its way through the Senate.[119] Senator John Rockefeller (D-W.Va.), Chairman of the Select Committee on Intelligence, favorably reported the bill out of his committee on October 26, 2007.[120] On October 31, the bill was referred to the Judiciary Committee which reported out a substitute amendment on November 16, 2007.[121] This Intelligence Committee version of the bill was more attuned to the Bush administration's ideas for permanent changes to FISA. It kept the PAA's definition of electronic surveillance, excluding "surveillance that is targeted . . . at a person reasonably believed to be located outside the United States" from the FISA definition of "electronic surveillance."[122] Additionally, like the PAA, the bill allowed the DNI and the AG to authorize targeting of persons reasonably believed to be outside the U.S. in

see also Ctr. for Democracy & Tech., Bills Would Strengthen, Weaken Surveillance Standards, Oct. 26, 2007, http://www.cdt.org/publications/policyposts/2007/13.

[112] H.R. 3773, 110th Cong. § 3 (2007) (as passed by House); *see also* Eric Lichtblau & Carl Huls, *Democrats Seem Ready to Extend Wiretap Powers*, N.Y. TIMES, Oct. 9, 2007, at A1.

[113] H.R. 3773, 110th Cong. § 4 (2007).

[114] *Id.* (requiring: a report to Congress within seven days of each application for or issuance of a FISA Court order for electronic surveillance; "regular audits" by the [Inspector General] of the [Department of Justice] to report to Congress on how electronic surveillance is affecting U.S. persons by reporting, among other things, "the number of targets of an acquisition under such order that were later determined to be located in the United States," and "compliance reports.").

[115] *Id.* § 11.

[116] *Id.* § 9.

[117] *Id.* § 18.

[118] Ctr. for Democracy & Tech., *supra* note 111, at 3. **R**

[119] S. 2248, 110th Cong. (2007).

[120] 153 CONG. REC. S13,489 (daily ed. Oct. 26, 2007).

[121] 153 CONG. REC. S14,618 (daily ed. Nov. 16, 2007).

[122] S. 2248, 110th Cong. § 701 (2007) (as reported by the S. Comm. on Intelligence).

order to acquire foreign intelligence information.[123] Like the PAA, these directives did not require a prior court order, and the FISA Court only had prior review over the procedures.[124] However, unlike both the PAA and the RESTORE Act, the Intelligence Committee version of the FISA Amendments Act required that all FISA Court orders to acquire communications of any U.S. citizen or resident who is abroad be based on probable cause.[125] Like the RESTORE Act, the Intelligence version provided for congressional oversight of the electronic surveillance program,[126] but it did not provide for an audit of the TSP by the Inspectors General. Also like the RESTORE Act, the Intelligence version states that FISA "shall be the exclusive means by which electronic surveillance and the interception of domestic, wire, oral or electronic communications may be conducted."[127] Finally, the FISA Amendments Act preempted state investigations[128] and explicitly provided immunity for electronic communication service providers "in connection with an intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007. . . ."[129] The Intelligence Committee version of the FISA Amendments Act was set to expire on December 31, 2013.[130]

The version of the FISA Amendments Act presented by the Judiciary Committee differed from version presented by Intelligence Committee in several respects. According to the Senate Judiciary Committee, "the PAA raised significant concerns because of its lack of any protection for or oversight of communications involving United States persons."[131] First, the Judiciary Committee did not adopt the altered definition of electronic surveillance, but it did allow the DNI and the AG jointly to authorize targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information for up to one year.[132] Unlike the Intelligence Committee bill, the Judiciary bill required a prior court order before a U.S. person abroad could be made the target of surveillance conducted domestically or abroad.[133] Like the RESTORE Act and the version of the FISA Amendment Acts submitted by the Intelligence Committee, the version submitted by the Judiciary Committee stated that FISA "shall be the exclusive means for targeting United States persons for the purpose of acquiring their

[123] *Id.* § 703. The FISA Amendments Act places additional limitations not contained in the PAA. Such acquisitions: (1) may not intentionally target persons known to be in the U.S.; (2) may not intentionally target a person outside the U.S. if the purpose is to target someone reasonably believed to be in the U.S.; and (3) shall comport with the Fourth Amendment. *Id.*

[124] *Id.* § 703(c)(3), (e)(2), (f)(2), (i).

[125] *Id.* § 703(c)(1),(2).

[126] *Id.* § 703(l).

[127] *Id.* § 102.

[128] S. 2248, 110th Cong. § 204 (2007) (as reported by the S. Comm. on Intelligence).

[129] *Id.* tit. II, § 202.

[130] *Id.* § 704.

[131] S. REP. NO. 110-258, at 3 (2007) (the Judiciary Committee bill passed 10 to 9).

[132] S. 2248, 110th Cong. § 702 (2007) (as reported by the S. Comm. on Judiciary).

[133] *Id.* § 702(a),(c)(2).

communications or communications information for foreign intelligence purposes, whether such persons are inside the United States or outside the U.S. except in cases where specific statutory authorization exists to obtain communications information without an order under this Act."[134] The Judiciary version of the FISA Amendments Act was scheduled to sunset on December 31, 2011.[135]

The Judiciary version of the FISA Amendments Act was tabled on January 24, 2008, by a vote of sixty to thirty-six.[136] On February 12, 2008, the Senate passed the Intelligence Version by a vote of sixty-eight to twenty-nine and incorporated it into the RESTORE Act by striking everything after the enacting clause and inserting the text of the Intelligence version of the FISA Amendments Act, with some minor amendments.[137] Notably, the incorporated version kept the PAA's definition of electronic surveillance, provided immunity to telecommunications providers, and did not require the Inspectors General to audit the TSP.

The House leadership decided not to vote on the Senate version of the RESTORE Act before the PAA expired on February 16, 2008, and let the PAA lapse before Congress went on a week-long recess.[138] Instead, the Democratic leadership sought to extend the PAA another 21 days, but that bill[139] failed 229-191.[140] The House tried to negotiate a compromise with the Senate.[141] However, on March 11, the House leadership announced that it was going to consider passing an alternative that would establish a bi-partisan commission to investigate the TSP and "allow phone companies to present a defense in a closed door U.S. district court, with the judge given access to confidential documents about electronic surveillance begun after the September 11 attacks."[142]

The Bush administration harshly criticized this new development in the House. First, it claimed that "the RESTORE Act could reopen dangerous intelligence gaps by imposing a cumbersome court approval process that would make it harder to collect intelligence on foreign terrorists."[143] Second, it criticized the fact that the RESTORE Act "fails to provide liability protec-

[134] *Id.* § 102.
[135] *Id.* § 703(c).
[136] *See* 154 CONG. REC. S227-256 (daily ed. Jan. 24, 2008) (roll call vote no. 2).
[137] 154 CONG. REC. S904 (daily ed. Feb. 12, 2008).
[138] *See* Robert D. Novak, *Why Torts Trumped Terrorism*, WASH. POST, Feb. 18, 2008, at A17.
[139] H.R. 5540, 110th Cong. (2008).
[140] *See* 154 CONG. REC. H906–907 (daily ed. Feb. 13, 2008) (roll call no. 54).
[141] Jay Rockefeller, Patrick Leahy, Silvestre Reyes & John Conyers, *Scare Tactics and Our Surveillance Bill*, WASH. POST, Feb. 25, 2008, at A15.
[142] Thomas Ferraro, *Democrats Seek Alternative on Phone Immunity*, WASH. POST, Mar. 11, 2008, *available at* http://www.reuters.com/article/politicsNews/idUSN1162638420080311.
[143] George W. Bush, Remarks on FISA, (Mar. 13, 2008) (transcript *available at* 2008 WL 670243).

tion to companies believed to have assisted in protecting our nation after the 9/11 attacks."[144]

As this Recent Development went to press, the House of Representatives held its first closed session in twenty-five years to debate the proposed amendments to FISA.[145] It passed the alternative to the Senate Bill by a vote of 221 to 188, thereby rejecting the Senate's grant of retroactive immunity.[146] The White House immediately objected to the vote, calling it "a significant step backward in defending our country against terrorism."[147] The White House went on to promise that President Bush would veto the bill if it passed the Senate.[148]

VI. CONCLUSION

The PAA attempted to modernize FISA and give the Executive Branch the tools it needs to wage the war on terror. To accomplish this goal, it altered the definition of electronic surveillance and provided the government new ways to authorize surveillance and the collection of foreign intelligence without a warrant. Scholars and policymakers continue to debate the tensions between the protections of the Fourth Amendment and the full extent of the President's power under Article II, as well as the implications of those tensions on a statutory scheme regulating electronic surveillance for foreign intelligence. But so long as Congress clearly states the rules governing these intelligence activities and the Executive Branch faithfully reports its compliance with those rules, the statute can once again be updated to meet the intelligence needs of the United States while respecting the privacy rights of its citizens.

Furthermore, whatever form FISA finally takes, Americans should be made aware of the degree to which warrantless surveillance affects them so that they can choose, through the political system, exactly where the balance between security and privacy should lie. The proposed bills in Congress took important steps toward transparency by providing for much more oversight than the PAA did.

Finally, there are grave implications of granting retrospective immunity to telecommunications service providers for their past transgressions. Regardless of whether Congress decides to grant retroactive immunity, it should carefully watch whether private companies are cooperating with the government when they should and standing up for their customers' privacy

---

[144] *Id.*

[145] Susan Crabtree & Walter Alarkon, *Hoyer Agrees to Closed FISA Session*, THE HILL, Mar. 13, 2008, *available at* http://thehill.com/leading-the-news/house-gop-seeks-closed-session-on-fisa-2008-03-13.html.

[146] Eric Lichtblau, *House Vote to Reject Immunity for Phone Companies Involved in Wiretaps*, N.Y. TIMES, Mar. 15, 2008, at A14.

[147] *Id.*

[148] *Id.*

rights when they should. If the companies do not seem to be adequately protecting their customers' privacy, Congress should consider providing incentives for telecommunications companies to comply with the law and protect the rights of their customers by challenging unlawful directives.

*—Juan P. Valdivieso**

* J.D. Candidate, Harvard Law School, Class of 2009; B.A., Princeton University, 2004.