RECENT LEGISLATION

ELECTRONIC SURVEILLANCE — CONGRESS GRANTS TELECOMMUNICATIONS COMPANIES RETROACTIVE IMMUNITY FROM CIVIL SUITS FOR COMPLYING WITH NSA TERRORIST SURVEILLANCE PROGRAM. — FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

In December 2005, the *New York Times* reported that President Bush had secretly authorized the National Security Agency (NSA) to eavesdrop without a warrant on people in the United States — including American citizens — for evidence of terrorist activity.[1] As part of the "terrorist surveillance program"[2] (TSP), the executive branch had "provided written requests or directives to U.S. electronic communication service providers to obtain their assistance with communications intelligence activities that had been authorized by the President."[3] After this information became public, over forty lawsuits were filed against a number of telecommunications companies for their alleged role in assisting the TSP; collectively, "these suits s[ought] hundreds of billions of dollars in damages."[4] The Bush Administration urged Congress to provide retroactive immunity for these companies;[5] civil liberties advocates and other groups opposed the idea.[6]

On July 10, 2008, Congress passed the FISA Amendments Act of 2008,[7] which provides blanket retroactive[8] immunity to telecommuni-

---

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

[2] John Diamond & David Jackson, *White House on Offense in NSA Debate*, USA TODAY, Jan. 24, 2006, at 10A.

[3] S. REP. NO. 110-209, at 9 (2007).

[4] *Id.* at 7. Normally, electronic communication service providers may only provide assistance in intelligence gathering activities if they are presented with either a court order or a written certification "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." 18 U.S.C. § 2511(2)(a)(ii) (2006).

[5] *See, e.g.*, Press Release, John M. McConnell, Dir. of Nat'l Intelligence, Modernization of the Foreign Intelligence Surveillance Act (FISA) (Aug. 2, 2007), *available at* http://www.dni.gov/press_releases/20070802_release.pdf ("[T]hose who assist the Government in protecting us from harm must be protected from liability.").

[6] *See, e.g.*, Letter from Caroline Fredrickson, Dir., Wash. Legislative Office, ACLU, & Michelle Richardson, Legislative Consultant, to the Senate (Feb. 4, 2008), http://www.aclu.org/safefree/general/33909leg20080204.html [hereinafter Fredrickson & Richardson] (urging Senators to "vote 'no' on final passage to any spying bill that . . . grants retroactive immunity to companies who broke the law by facilitating illegal spying"); Letter from MoveOn.org Political Action Team to MoveOn Members (June 21, 2008), http://pol.moveon.org/immunity/080621obama.html (urging members to call Senator Barack Obama to "[a]sk him to block any compromise that includes immunity for phone companies that helped Bush break the law").

[7] Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

[8] FISA already provided for *prospective* civil immunity for private parties that assist with electronic surveillance, so long as they do it under the auspices of the statutory framework.

cations companies that assisted the TSP.[9] This provision allows the Attorney General to immunize these private parties from suit by certifying that the President requested their assistance and assured them that their actions were legal.[10] The provision undermines both the statutory scheme of the Foreign Intelligence Surveillance Act of 1978[11] (FISA) and Congress's role in striking the proper balance between national security and civil liberties. Although proponents argued that blanket immunity was necessary to protect telecommunications companies from unfair penalties and to encourage their compliance in the future,[12] an amendment proposed by Senator Arlen Specter[13] would have addressed these concerns while reducing some of the problems associated with the blanket immunity provision. Congress should have passed Senator Specter's amendment rather than the blanket immunity provision that it ultimately enacted.[14]

The first version of the bill, entitled the RESTORE Act of 2007,[15] was introduced in the House by Representative John Conyers on October 9, 2007.[16] This bill did not provide for any retroactive immunity.[17] After extensive debate, the House passed the bill on November 15.[18] Meanwhile, on October 26, the Senate Select Committee on Intelligence reported an original bill entitled the FISA Amendments Act of 2007,[19] which contained a provision for retroactive immunity similar to the provision that was ultimately enacted.[20] The Intelligence

---

See 50 U.S.C. § 1805(i) (2000) ("No cause of action shall lie in any court against any . . . person . . . that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance . . . .").

9 *See* FISA Amendments Act of 2008 § 201, 122 Stat. at 2468–70 (adding § 802 to FISA).

10 *See id.* § 201, 122 Stat. at 2468–69 (adding § 802(a) to FISA).

11 Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

12 *See, e.g.*, Letter from Michael B. Mukasey, Att'y Gen., & J.M. McConnell, Dir. of Nat'l Intelligence, to Nancy Pelosi, Speaker, U.S. House of Representatives (June 19, 2008) [hereinafter Mukasey & McConnell], *available at* http://www.lifeandliberty.gov/docs/ag-dni-fisa-letter061908.pdf.

13 *See* 154 CONG. REC. S712 (daily ed. Feb. 6, 2008) (statement of Sen. Specter).

14 Senator Specter's amendment was not the only proposed compromise. For example, Senator Dianne Feinstein proposed providing immunity for telecommunications companies only after a finding by the FISA court that a company received a written directive from the Administration certifying that compliance was lawful and that the company had held an "objectively reasonable belief under the circumstances that compliance with the written request or directive was lawful." *Id.* at S707. These compromises sought to provide protection for companies that reasonably believed that they were complying with the law, without effectively authorizing the President to use private parties to circumvent the law.

15 H.R. 3773, 110th Cong. (2007).

16 *Id.*

17 153 CONG. REC. H11,663 (daily ed. Oct. 17, 2007) (statement of Rep. Conyers).

18 *Id.* at H14,062 (daily ed. Nov. 15, 2007). The bill passed by a vote of 227 to 189. *Id.*

19 S. 2248, 110th Cong. (as reported by S. Comm. on Intelligence, Oct. 26, 2007).

20 *See id.* tit. II.

Committee report stated that the bill extended retroactive immunity to telecommunications companies because "they acted in good faith and should be entitled to protection from civil suit."[21] On November 16, the Senate Committee on the Judiciary reported a different version of the bill,[22] which "d[id] not include . . . blanket retroactive immunity."[23] However, the Senate voted to table the Judiciary Committee bill,[24] leaving the Intelligence Committee bill as the sole version under consideration in the Senate.

Senator Specter subsequently proposed an amendment that would "substitute the U.S. Government as a party defendant for the telephone companies," thereby shielding them from liability while still allowing courts to rule on the legality of the TSP and the constitutional questions raised by the President's assertions of executive authority.[25] Government substitution would be dependent upon a finding by the FISA court that the telecommunications companies acted "in good faith."[26] The Senate rejected this amendment by a vote of sixty-eight to thirty.[27] Ultimately, the Senate passed the bill and sent it back to the House with the blanket immunity provision intact.[28]

On June 19, 2008, Representative Silvestre Reyes introduced the FISA Amendments Act of 2008[29] in the House.[30] This bill was substantially the same as the version passed by the Senate.[31] On June 20, the House voted to pass the bill.[32] The Senate subsequently considered the House bill and rejected three more amendments that would have altered or eliminated the retroactive immunity provision.[33] On July 9, the Senate passed the House bill by a vote of sixty-nine to twenty-eight.[34] The President signed the bill into law the next day.[35]

The final version of the immunity provision states that courts should dismiss any suit against an electronic service provider alleged

---

[21] S. REP. NO. 110-209, at 10 (2007).

[22] 153 CONG. REC. D1537 (daily ed. Nov. 15, 2007). The Judiciary Committee offered "an amendment in the nature of a substitute." *Id.*

[23] S. REP. NO. 110-258, at 4 (2008).

[24] 154 CONG. REC. S255–56 (daily ed. Jan. 24, 2008). Senator Kit Bond moved to table the amendment; this motion passed by a vote of 60 to 36. *Id.*

[25] *Id.* at S712 (daily ed. Feb. 6, 2008) (statement of Sen. Specter).

[26] *Id.* at S713 (statement of Sen. Whitehouse).

[27] *Id.* at S889 (daily ed. Feb. 12, 2008).

[28] *Id.* at S904. The Senate passed S. 2248 by a vote of 68 to 29. *Id.*

[29] H.R. 6304, 110th Cong. (2008).

[30] 154 CONG. REC. H5728 (daily ed. June 19, 2008).

[31] *Compare* H.R. 6304, *with* H.R. 3773, 110th Cong. (2008) (as passed by the Senate, Feb. 12, 2008).

[32] 154 CONG. REC. H5774 (daily ed. June 20, 2008). The bill passed by a vote of 293 to 129. *Id.*

[33] *Id.* at S6469–70 (daily ed. July 9, 2008).

[34] *Id.* at S6476.

[35] *Id.* at D876 (daily ed. July 11, 2008).

to have provided assistance "in connection with an intelligence activity involving communications that was . . . designed to detect or prevent a terrorist attack . . . against the United States"[36] if the Attorney General certifies that one of two conditions is met. Suits should be dismissed if the Attorney General certifies either that the company was acting pursuant to a "written request or directive" from the government indicating that such activity was "(i) authorized by the President; and (ii) determined to be lawful,"[37] or else that the company "did not provide the alleged assistance."[38] The Act provides for a "substantial evidence" standard for judicial review of the Attorney General's certifications.[39] Additionally, the Act provides that courts may limit public disclosure of any certification or supplemental materials that would prove harmful to national security.[40]

The blanket immunity provision retroactively validates presidential directives to private parties that ordered them to conduct potentially illegal actions.[41] This result is problematic for several reasons. First, it undermines the statutory framework that Congress originally established in FISA. Second, it undermines the ability of Congress to play a meaningful role in determining the proper procedures for gathering intelligence, as it weakens the requirement that the Administration get statutory approval before fundamentally changing surveillance policy. Finally, it greatly reduces the chances that a court will be able to review the legality of the TSP and the constitutionality of the President's assertions of executive authority. Proponents of the blanket immunity provision argued that it was necessary for a number of reasons, including fairness and national security.[42] However, the amendment pro-

---

[36] FISA Amendments Act of 2008 § 201, 122 Stat. at 2468–69 (adding § 802(a)(4)(A) to FISA).

[37] *Id.* § 201, 122 Stat. at 2469 (adding § 802(a)(4)(B) to FISA).

[38] *Id.* (adding § 802(a)(5) to FISA).

[39] *Id.* (adding § 802(b)(1) to FISA).

[40] *Id.* (adding § 802(c) to FISA).

[41] The question of whether the TSP was in fact legally justified is still open to debate, as the Supreme Court has not ruled directly on this issue. The Administration's legal justifications are at the very least of questionable merit. *See* Curtis Bradley et al., *On NSA Spying: A Letter to Congress*, N.Y. REV. BOOKS, Feb. 9, 2006, at 42; *see also* Memorandum from Elizabeth B. Bazan & Jennifer K. Elsea, Legislative Att'ys, Cong. Research Serv. Am. Law Div., to Members of Congress 42–44 (Jan. 5, 2006), *available at* http://www.fas.org/sgp/crs/intel/m010506.pdf [hereinafter Bazan & Elsea] (stating that although the legality of the NSA program is "impossible to determine without an understanding of the specific facts involved," *id.* at 42–43, it nevertheless appears that "the Administration's legal justification . . . does not seem to be as well-grounded" as the Administration had suggested, *id.* at 44).

[42] *See, e.g.*, Mukasey & McConnell, *supra* note 12, at 3–4 ("Providing this liability protection is critical to the Nation's security. As the Senate Select Committee on Intelligence recognized, 'the intelligence community cannot obtain the intelligence it needs without assistance from [the telecommunications] companies.' That committee also recognized that companies in the future may be less willing to assist the Government if they face the threat of private lawsuits each time they

posed by Senator Specter would have addressed most of these concerns while avoiding many of the problems of the blanket immunity provision. Congress should have adopted this amendment instead.

When Congress enacted FISA, it attempted to establish a clear and exclusive framework for all parties to follow when the government seeks the aid of private companies in conducting electronic surveillance.[43] Members of the Bush Administration appear to have acknowledged that the TSP operated outside this statutory framework,[44] but they argue that the TSP was nevertheless legally justified both by the Authorization for Use of Military Force[45] (AUMF) passed by Congress in 2001 and by the President's inherent authority under Article II of the Constitution.[46] The blanket immunity provision undermines FISA by granting retroactive immunity to telecommunications companies without requiring any showing that they reasonably believed that assisting the intelligence agencies was legal;[47] the Attorney General merely has to certify that the company was told by the government that its actions were legal.[48] Since the Administration appears to have based its legal reasoning upon executive authority rather than compliance with FISA,[49] neither the companies nor the President needed to believe they were complying with FISA in order for the companies to receive immunity. Congress has therefore allowed the Administration and private companies to act outside of the statutory framework that Congress created. The effectiveness of FISA as a comprehensive scheme governing electronic surveillance is undermined if the President can circumvent its procedures simply by asserting that he has the executive authority to act outside of its framework. FISA's effectiveness will be further undermined if telecommunications companies are willing to cooperate with intelligence agencies even when FISA procedures have not been followed.

---

are believed to have provided assistance. Finally, allowing litigation over these matters risks the disclosure of highly classified information regarding intelligence sources and methods.").

[43] *See* 18 U.S.C. § 2511(2)(f) (2006) (The procedures listed in FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted.").

[44] *See, e.g.*, Press Briefing, Alberto Gonzales, Att'y Gen., & Gen. Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html ("I can say unequivocally that we have used [the TSP] in lieu of [the FISA process] and this program has been successful.").

[45] Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 note (Supp. V 2005)).

[46] For more on the Administration's arguments, see Bazan & Elsea, *supra* note 41, at 27–42.

[47] By contrast, the Specter amendment would have required a company to have had a good faith belief that its actions were legal in order to receive immunity. *See* 154 CONG. REC. S713 (daily ed. Feb. 6, 2008) (statement of Sen. Whitehouse).

[48] FISA Amendments Act of 2008 § 201, 122 Stat. at 2469 (adding § 802(a)(4)(B) to FISA).

[49] *See* Bazan & Elsea, *supra* note 41, at 27–42.

Furthermore, as the intelligence community increasingly relies on the help of private companies to conduct electronic surveillance, it is essential that a range of government actors — including Congress — gets to weigh in on important policy considerations, including the proper balance between individual privacy rights and national security.[50] Congress can and should serve as a check on the executive, as the executive branch may be "institutionally predisposed" to value security over civil liberties.[51] It is therefore important that Congress establish the proper procedures for the Administration to follow when it works with the private sector to conduct electronic surveillance, and that Congress then makes sure that these procedures are followed. When the Administration and private parties act outside of the statutory framework, they should pay a price, even if Congress would have approved of their actions had its approval been sought; in this case, that price should be civil liability. There is nothing wrong with Congress changing FISA at the request of the Administration; in other provisions of the Act, Congress does just that — it updates and changes the procedures for conducting electronic surveillance.[52] However, in order for Congress to play a meaningful role in determining surveillance policy, the Administration should have to seek Congress's approval *before* making a major policy change and acting outside the statutory framework. Despite its intention to limit extralegal arrangements, Congress has signaled to both the Administration and the telecommunications companies that they can ignore the statutory framework without suffering adverse consequences. As a result, the Administration is likely to rely more on informal agreements with telecommunications companies,[53] and Congress's role in making policy and providing oversight will be diminished.

Finally, the blanket immunity provision will also likely prevent any judicial rulings on the underlying legal issues at stake.[54] No court will

---

[50] *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 904–05 (2008); *see also id.* at 932–35.

[51] *Id.* at 903; *see also* Hamdi v. Rumsfeld, 542 U.S. 507, 545 (2004) (Souter, J., concurring in part, dissenting in part, and concurring in the judgment) ("[D]eciding finally on what is a reasonable degree of guaranteed liberty . . . is not well entrusted to the Executive Branch of Government, whose particular responsibility is to maintain security. . . . [T]he branch of the Government asked to counter a serious threat is not the branch on which to rest the Nation's entire reliance in striking the balance between the will to win and the cost in liberty on the way to victory; the responsibility for security will naturally amplify the claim that security legitimately raises. A reasonable balance is more likely to be reached on the judgment of a different branch . . . .").

[52] *See* FISA Amendments Act of 2008 §§ 101–110, 122 Stat. at 2437–67.

[53] *See* Michaels, *supra* note 50, at 910–12 (discussing these informal arrangements in the context of the TSP).

[54] EDWARD C. LIU, CONG. RESEARCH SERV., CRS REPORT FOR CONGRESS: RETROACTIVE IMMUNITY PROVIDED BY THE FISA AMENDMENTS ACT OF 2008, at 2 (2008), *available at* http://www.fas.org/sgp/crs/intel/RL34600.pdf.

be able to determine the validity of the Administration's argument that the President has the inherent constitutional authority to conduct electronic surveillance without congressional approval and that this authority is supplemented by the AUMF.[55] Regardless of whether the Administration's arguments would hold up in court, a decision one way or the other would provide more certainty to all parties involved: the Administration would know whether it has to follow FISA under all circumstances; Congress would know to what extent it can limit the President's ability to conduct surveillance; and the telecommunications companies would know whether they can rely on the Administration's assertions that providing assistance is legal. Also, since any pending lawsuits will almost certainly be dismissed, individuals whose privacy rights were violated will be unable to vindicate those rights in court.[56]

Because of these problems, Congress should not have enacted the blanket immunity provision unless it was absolutely necessary, which it was not. Proponents of blanket immunity argued that it was necessary both to prevent unfairly punishing telecommunications companies that tried to assist the government in preventing another terrorist attack[57] and to ensure the cooperation of telecommunications companies in the future.[58] However, the amendment proposed by Senator Specter would have accomplished both of these goals while avoiding some of the problems inherent in the blanket immunity provision. Under this amendment, any telecommunications company that complied with the government *and acted in good faith* would be shielded from liability. If the FISA court found that a company did act in good faith, then the government would take its place in any lawsuits.[59] According to Senator Sheldon Whitehouse, it would be proper to hold the government accountable because "if the companies acted reasonably and in good faith at the direction of the Government but ended up breaking the law, the Government truly is the morally proper party to the case."[60] Furthermore, some companies had threatened that if they were not given immunity, they would refuse to cooperate with the government in the future "except under strict compulsion."[61] The Specter amendment would enable most carriers to escape liability through a showing

---

55 *See* Bazan & Elsea, *supra* note 41, at 27 (discussing the Administration's argument).

56 Fredrickson & Richardson, *supra* note 6. Similar lawsuits against the government have already proved unsuccessful. *See* ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 128 S. Ct. 1334 (2008).

57 *See, e.g.*, Press Release, John M. McConnell, *supra* note 5.

58 *See, e.g.*, Mukasey & McConnell, *supra* note 12, at 3–4.

59 See Federal Rule of Civil Procedure 25(c) for the procedure on substitution of parties.

60 154 CONG. REC. S713 (daily ed. Feb. 6, 2008) (statement of Sen. Whitehouse); *see also* SENATE REPUBLICAN POLICY COMM., FISA MODERNIZATION AND CARRIER LIABILITY 3 (2008).

61 SENATE REPUBLICAN POLICY COMM., *supra* note 60, at 3.

of good faith, thereby providing them with the desired immunity and encouraging their future cooperation.

In addition to addressing many of the concerns of the proponents of blanket immunity, the Specter amendment would also have reduced some of the problems caused by the blanket immunity provision. First, by protecting companies only after a judicial finding that they acted in reasonable good faith, Congress would have sent a clear signal to private companies that they must determine for themselves whether a government request for assistance is legal. Congress would also have sent a message to the President that he cannot ignore existing statutes and authorize private parties to commit potentially unlawful actions without being subjected to intense judicial scrutiny. Congress would therefore have encouraged both the Administration and the private sector to comply with FISA. As a result, Congress would have reasserted its role in determining the proper surveillance procedures by holding parties accountable for circumventing those procedures. The Specter amendment may also have allowed courts to rule directly on the legality of several aspects of the TSP. Finally, the amendment would have given private citizens the "ability to vindicate their rights in court regarding wiretapping abuses of the past."[62]

Senator Specter's amendment presented Congress with an opportunity to encourage both the executive branch and the private sector to follow the law, to provide some accountability for what appear to be extensive violations of the law, and to reassert itself as an important player in the debate over how to conduct electronic surveillance. Congress could have achieved these goals without making any major sacrifices in terms of fairness or national security. Yet Congress, at the behest of the Administration and the telecommunications industry, instead chose to provide blanket immunity to the telecommunications companies and virtually ensure that important legal questions about the TSP will remain unanswered.[63] Although it is important to encourage cooperation between telecommunications companies and the intelligence agencies, it is also important for Congress to play a role in determining the proper balance between security and civil liberties rather than leaving such a determination to the Administration.[64] By allowing the Administration and telecommunications companies to ignore FISA with impunity, Congress has abdicated this responsibility.

---

[62] Fredrickson & Richardson, *supra* note 6.

[63] *See* LIU, *supra* note 54, at 2.

[64] *See* Michaels, *supra* note 50, at 903 & n.5.