Order Code RL34279

CRS Report for Congress

The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues

Updated December 14, 2007

Elizabeth B. Bazan
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues

Summary

The current legislative and oversight activity with respect to electronic surveillance under Foreign Intelligence Surveillance Act (FISA) has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need identified by the Director of National Intelligence (DNI), Admiral Mike McConnell, for the Intelligence Community to be able to efficiently and effectively collect foreign intelligence information from the communications of foreign persons located outside the United States in a changing, fast paced, and technologically sophisticated international environment, and the differing approaches suggested to meet this need; and limitations of liability for those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments.

Congress currently has before it several bills that, if enacted, would amend certain FISA provisions, among them H.R. 3733, which was passed by the House on November 15, 2007; S. 2248 (as reported out of the Senate Select Committee on Intelligence); and S. 2248 (as reported out of the Senate Judiciary Committee with an amendment in the nature of a substitute). Two other bills regarding FISA were introduced by Senator Reid on December 10, 2007, and have been placed on the Senate's legislative calendar, S. 2440 and S. 2441. S. 2402, introduced by Senator Specter on December 3, 2007, was referred to the Senate Judiciary Committee. In Committee markup on December 13, 2007, an amendment in the nature of a substitute to S. 2402 was adopted by unanimous consent. Then, by a vote of 5-13, the Committee rejected S. 2402, as amended. The proposal would have permitted substitution of the government for electronic communication service providers in law suits where certain criteria were met.

This report briefly examines these issues and sets them in context. For a side-by-side comparison of H.R. 3773 and the two reported versions of S. 2248, see CRS Report RL34277, *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*, by Elizabeth B. Bazan (December 6, 2007).

Contents

Tension Between National Security and Civil Liberties 3

Collection of Foreign Intelligence Information from Foreign Persons Located Abroad 7

Limitations on Liability for Telecommunications Providers Furnishing Aid to the Government 12

The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues

The Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, 92 Stat. 1783 (October 25, 1978), 50 U.S.C. §§ 1801 *et seq*. (hereinafter FISA), was enacted in response both to the Committee to Study Government Operations with Respect to Intelligence Activities (otherwise known as the Church Committee) revelations regarding past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the subject.[1] While FISA now provides

---

[1] The U.S. Supreme Court originally held that the Fourth Amendment only applied to tangible things, Olmstead v. United States, 277 U.S. 438 (1928). but later held that intangible things, such as conversations, were also protected. In its 1967 decision in Katz v. United States, 389 U.S. 347, 353, 359 n. 23 (1967), the Court, overturning its previous holding in Olmstead v. United States, held that the Fourth Amendment covered electronic surveillance of oral communications without physical intrusion. The *Katz* Court stated, however, that its holding did not extend to cases involving national security. In United States v. United States District Court, 407 U.S. 297, 313-14 (1972) (the Keith case), the Court regarded *Katz* as "implicitly recogniz[ing] that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." Mr. Justice Powell, writing for the *Keith* Court, framed the matter before the Court as follows:

> The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.

407 U.S. at 299. The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment. Justice Powell emphasized that the case before it "require[d] no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country." *Id*., at 308 The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents." *Id.*, at 321-22. However, the guidance which the Court provided in *Keith* with respect to national security surveillance in a domestic context to some degree presaged the approach Congress was to take in foreign intelligence surveillance. *Id.* at 323-24.

Court of appeals decisions following *Keith* met more squarely the issue of warrantless

(continued...)

a statutory framework for gathering foreign intelligence information through the use of electronic surveillance, physical searches, and pen registers or trap and trace devices, and access to business records and other tangible things, the 1978 Act dealt only with electronic surveillance. The provisions passed almost 30 years ago became Title I of FISA. As originally enacted, the measure provided a statutory framework for collection of foreign intelligence information through the use of electronic surveillance of communications of foreign powers or agents of foreign powers, as those terms were defined in the act. The act has been amended repeatedly in the intervening years in an effort to address changing circumstances. Then, as now, the Congress sought to strike a balance between national security interests and civil liberties.

A number of FISA bills have received recent attention in the 110th Congress. The House of Representatives passed H.R. 3773 on November , while S. 2248 was reported out of the Senate Select Committee on Intelligence and an amendment in the nature of a substitute to S. 2248 was reported out of the Senate Judiciary Committee. Senator Reid introduced two additional FISA bills on December 10, 2007, S. 2440 and S. 2441, which were read twice the following day and placed on the Senate Legislative Calendar as Numbers 529 and 530, respectively. S. 2402 was introduced by Senator Specter on December 3, 2007, and referred to the Senate Judiciary Committee. In Committee markup on December 13, 2007, an amendment in the nature of a substitute to S. 2402 was adopted by unanimous consent. Then, by a vote of 5-13, the Committee rejected S. 2402, as amended. The proposal would have permitted substitution of the government for electronic communication service providers in law suits where certain criteria were met.

The current legislative and oversight activity with respect to electronic surveillance under FISA has drawn national attention to several overarching issues. This report briefly outlines three such issues and touches upon some of the

---

[1] (...continued)
electronic surveillance in the context of foreign intelligence gathering. In United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974), the Fifth Circuit upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of Brown, an American citizen, was incidentally overheard. The Third Circuit in United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom*, Ivanov v. United States, 419 U.S. 881 (1974), concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information. In its plurality decision in Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976), the District of Columbia Circuit took a somewhat different view in a case involving a warrantless wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power. Finding that a warrant was required in such circumstances, the plurality also noted that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." For more information on the background of FISA, see CRS Report RL30465, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and U.S. Foreign Intelligence Surveillance Court and U.S. Foreign Intelligence Surveillance Court of Review Decisions*, by Elizabeth B. Bazan (February 15, 2007).

perspectives reflected in the ongoing debate. These issues include the inherent and often dynamic tension between national security and civil liberties, particularly rights of privacy and free speech; the need identified by the Director of National Intelligence (DNI), Admiral Mike McConnell, for the Intelligence Community to be able to efficiently and effectively collect foreign intelligence information from the communications of foreign persons located outside the United States in a changing, fast paced, and technologically sophisticated international environment,[2] and the differing approaches suggested to meet this need; and limitations of liability for those electronic communication service providers who furnish aid to the federal government in its foreign intelligence collection. This report briefly examine these issues and sets them in context.

Tension Between National Security and Civil Liberties

Two constitutional provisions, in particular, are implicated in this debate — the Fourth and First Amendments. The Fourth Amendment to the U.S. Constitution 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 Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

---

[2] *See* Statement of the Director of National Intelligence, Subject: Modernization of the Foreign Intelligence Surveillance Act (FISA) (August 2, 2007), stating in pertinent part:

> First, the Intelligence Community should not be required to obtain court orders to effectively collect foreign intelligence from foreign targets located overseas. Simply due to technology changes since 1978, court approval should not now be required for gathering intelligence from foreigners located overseas. This was not deemed appropriate in 1978 and it is not appropriate today. . . .
>
> The Intelligence Community should not be restricted to effective collection of only certain categories of foreign intelligence when the targets are located overseas. We must ensure that the Intelligence Community can be effective against all who seek to do us harm.
>
> The bill must not require court approval before urgently needed intelligence collection can begin against a foreign target located overseas. The delays of a court process that requires judicial determinations in advance to gather vital intelligence from foreign targets overseas can in some cases prevent the rapid gathering of intelligence necessary to provide warning of threats to the country. This process would also require in practice that we continue to divert scarce intelligence experts to compiling these court submissions. Similarly, critical intelligence gathering on foreign targets should not be halted while court review is pending.
>
> . . . .

This statement may be found at [http://www.odni.gov/press_releases/200708002_release.pdf].

The First Amendment to the U.S. Constitution provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

As the Fourth Amendment protects the people's privacy rights, so the First Amendment reflects a recognition of the value of free expression of ideas and lawful political dissent to the preservation of a free society.

In introducing S. 1566, the bill that became the Foreign Intelligence Surveillance Act of 1978, P.L. 95-511, Senator Edward Kennedy addressed the challenge of striking an appropriate balance between the legitimate government need to safeguard the nation against the intelligence activities of foreign agents and the concomitant need to protect civil liberties, stating:

> The complexity of the problem must not be underestimated. Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens. My objective over the past six years has been to reach some kind of fair balance that will protect the security of the United States without infringing on our citizens' human liberties and rights.[3]

This sentiment was echoed in a hearing before the Senate Judiciary Committee on S. 1566 when Attorney General Griffin Bell testified for the Carter Administration in favor of the measure:

> I believe this bill is remarkable not only in the way it has been developed, but also in the fact that for the first time in our society the clandestine intelligence activities of our government shall be subject to the regulation and receive the positive authority of a public law for all to inspect. President Carter stated it very well in announcing this bill when he said that "one of the most difficult tasks in a free society like our own is the correlation between adequate intelligence to guarantee our nation's security on the one hand, and the preservation of basic human rights on the other." It is a very delicate balance to strike, but one which is necessary in our society, and a balance which cannot be achieved by sacrificing either our nation's security or our civil liberties. . . .[4]

---

[3] Report of the Senate Committee on the Judiciary to accompany S. 1566, S.Rept. 95-604, Part I, 95th Cong., 1st Sess. 8 (1977); 1978 U.S.C.C.A.N. 3904, 3910. FISA was enacted in the wake of revelations of abuses of warrantless surveillance in the name of national security revealed in the 1973 investigation of the Watergate break-ins and later explored in greater detail by Church Committee. *Id.* at 7, 1978 U.S.C.C.A.N. at 3908. See also, Foreign Intelligence Surveillance Act of 1978, H.Rept. 95-1283, Part I, 95th Cong., 2d Sess. 14 (1978).

[4] Hearing before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, Foreign Intelligence Surveillance Act of 1977, 95th Cong., 1st Sess. 23 (1977).

In providing background for its report on H.R. 7308, the House FISA bill then under consideration, the House Permanent Select Committee on Intelligence noted:

> The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an "inherent power" to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades.[5]

Electronic surveillance can provide vital information needed to identify those who are acting or preparing to act against U.S. interests for the benefit of foreign powers, including those engaged in espionage, sabotage, or terrorist acts or who otherwise pose a threat to the nation or its citizens, and to uncover their plans or activities. This information may not be readily uncovered by other investigative means. Thus, surveillance can provide a valuable tool for protecting the security of the nation and its citizens. However, this investigative technique, by its nature, can intrude into the privacy of both the target of the surveillance and those with whom the target communicates. It also has the potential of chilling political discussion and lawful dissent.[6]

---

[5] Report of the House Permanent Select Committee on Intelligence to accompany H.R. 7308, the Foreign Intelligence Surveillance Act of 1978, H.Rept. 95-1283, Part I, 95th Cong., 2d Sess. 15 (1978).

[6] *See*, S.Rept. 95-604, at 8, 1978 U.S.C.C.A.N. 3909-3910. The Senate Judiciary Committee noted that "[i]n summarizing its conclusion that surveillance was "often conducted by illegal or improper means," the Church committee wrote:

> Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . . [P]ast subjects of these surveillances have included a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security, such as two White House domestic affairs advisers and an anti-Vietnam War protest group. (vol 2, p. 12)
>
> * * * *
>
> The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information — unrelated to any legitimate government interest — about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials. (vol. 3, p. 32)

(continued...)

The framing of the current debate on this issue flows, in part, from questions arising with respect to the Terrorist Surveillance Program (TSP), first revealed in press accounts in December 2005.[7] While little information regarding the details of this NSA program is publicly available, the President has indicated that, "since shortly after September 11, 2001, he had authorized the National Security Agency (NSA) to intercept international communications into and out of the United States of persons linked to al Queda or related terrorist organizations. The purpose of the intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States."[8] Concerns surrounding the TSP have led to continuing congressional oversight and a number of legislative proposals focused upon providing the intelligence community with the tools it needs for foreign

---

[6] (...continued)
The Senate Judiciary Committee observed further:

> Also formidable — although incalculable — is the "chilling effect" which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.

See also, Keith, 407 U.S. at 391-321, where Justice Powell observed that,

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power," *Marcus v. Search Warrant*, 367 U.S. 717, 724 (1961). . . . Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." . . . .

[7] *See, e.g.*, James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, December 16, 2005, at 1, 22 (citing anonymous government officials to report that the executive order, which allows some warrantless eavesdropping on persons inside the United States, "is based on classified legal opinions that assert that the president has broad powers to order such searches, derived in part from the September 2001 Congressional resolution authorizing him to wage war on Al Qaeda and other terrorist groups").

[8] "Legal Authorities Supporting the Activities of the National Security Agency Described by the President," U.S. Department of Justice (January 19, 2006). This may be found at [http://www.usdoj.gov/ag/readingroom/surveillance9.pdf].

intelligence collection to protect the United States and its citizens, while also protecting the civil liberties of those impacted by such collection.

The current level of complexity and sophistication of global communications technology can provide both increased opportunities for lawful private communications and public debate, and increased means for communications between those engaged in criminal wrongdoing or plans or actions which pose a threat to U.S. national security. While this presents challenges to intelligence collection for foreign intelligence purposes, the government has moved to utilize these new technologies for both law enforcement and intelligence purposes. The balance between these important governmental needs and protections of constitutionally protected privacy interests and First Amendment protected activities is dynamic, and there can be differences of opinion as to where the appropriate balance point between them may be found.

Collection of Foreign Intelligence Information from Foreign Persons Located Abroad

A second, related issue in the current debate concerns the appropriate circumstances or standards for collection of foreign intelligence information from foreign persons abroad. This issue can best be understood when set in the context of recent developments, to the extent that pertinent information is publicly available.

In July 2007, an unclassified summary of the National Intelligence Estimate (NIE) on "The Terrorist Threat to the US Homeland" was released. The NIE expressed the judgement, in part, that the U.S. Homeland will face a persistent and evolving threat over the next three years, the main threat coming from Islamic terrorist groups and cells, particularly al Qaeda.[9]

In a January 17, 2007, letter to Chairman Leahy and Ranking Member Specter of the Senate Judiciary Committee, then Attorney General Gonzales advised them that, on January 10, 2007, a Foreign Intelligence Surveillance Court judge "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." The Attorney General stated that, in light of these orders, which "will allow the necessary speed and agility," all surveillance previously occurring under the Terrorist Surveillance Program (TSP) would now be conducted subject to the approval of the FISC. He indicated further that, under these circumstances, the President had determined not to reauthorize the TSP when the then current authorization expired. The Attorney General also noted that the Intelligence Committees had been briefed on the highly classified details of the FISC orders and advised Chairman Leahy and Senator Specter that he had directed the Acting Assistant Attorney General for the Office of Legal Counsel and the Assistant

---

[9] National Intelligence Estimate on "The Terrorist Threat to the US Homeland," at 6-7 (July 2007). This may be found at [http://www.odni.gov/press_releases/20070717_release.pdf].

Attorney General for National Security to provide them a classified briefing on the details of the orders. Because the contents of these orders remain classified, the scope of or limitations with respect to any authority that may have been provided remain unknown.

On April 13, 2007, the Administration announced that it had submitted draft legislation to the Congress regarding modernization of FISA. This draft legislation included a proposed new section 102A of FISA which would authorize the President, acting through the Attorney General, to permit acquisition of foreign intelligence information for up to one year concerning persons reasonably believed to be outside the United States if the Attorney General certifies in writing under oath that he has made four specific determinations.[10]

On August 2, 2007, the DNI released a statement on "Modernization of the Foreign Intelligence Surveillance Act." In his statement, Admiral McConnell regarded such modernization as necessary to respond to technological changes and to meet the Nation's current intelligence collection needs. He viewed it as essential for the Intelligence Community to provide warning of threats to the United States. One of two critically needed changes perceived by the DNI was his view that a court order should not be required for gathering foreign intelligence from foreign targets located overseas. Admiral McConnell did, however, indicate that he would be willing to agree to court review, after commencement of needed collection, of the procedures by which foreign intelligence is gathered through classified methods directed at foreigners outside the United States.

Some news accounts suggest that a FISC court ruling this Spring may have limited the authority of the United States, in certain circumstances, to engage in surveillance of foreign conversations taking place outside the United States. Admiral McConnell stated in remarks included in the transcript of an interview published in the *El Paso Times* on August 22, 2007, that on or about May of this year, when another judge of the FISC considered an application for renewal or extension of the surveillance approved under the January 10 orders, that judge interpreted the requirements of FISA differently from the judge who had issued the January 10

---

[10] These include: that "the acquisition does not constitute electronic surveillance; that the acquisition involves obtaining foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;" that "a significant purpose of the acquisition is to obtain foreign intelligence information;" and that "the minimization procedures to be used with respect to the acquisition activity meet the definition of minimization procedures under section 101(h)" of FISA. The Fact Sheet on the draft legislation may be found at [http://www.usdoj.gov/opa/pr/2007/April/07_nsd_247.html]. The text of the draft bill may be found at [http://www.lifeandliberty.gov/docs/text-of-dni-proposed.pdf]. For further information about the proposed draft legislation regarding modernization of FISA, see the April 23, 2007, CRS Congressional Distribution Memorandum entitled, "Overview of 'FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization,'" by Elizabeth B. Bazan.

orders, and deemed a FISA warrant necessary for surveillance of wire communications of a foreign person in a foreign country.[11]

On August 5, 2007, the Protect America Act of 2007 was enacted, P.L. 110-55, which provided that "[n]othing in the definition of electronic surveillance under section 101(f) [of FISA] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States." It also created a new procedure under section 105B(a) of FISA under which the Attorney General and the DNI, for periods of up to one year, may authorize acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, if the Attorney General and the DNI determine, based on the information provided to them, that five criteria have been met.[12] This authority is similar, but not identical to, the proposed section 102A of FISA in the Administration's draft bill.

Views differ as to the scope of the need and the means by which this need may be met. Can this concern be addressed by solutions directed solely at electronic surveillance or acquisitions without a court order from the FISC of communications between foreign persons in communication with other foreign persons all located outside the United States, whether or not those communications are routed through the United States at some point in their transmission? Or must the solution be crafted in such a way as to permit such surveillance or acquisitions of the communications of foreign persons located abroad, whether they may be in communication only with other non-U.S. persons, or both non-U.S. persons and U.S. persons,[13] located outside the United States? What is required if some of the communications of the foreign person targeted in the surveillance or acquisition are with U.S. persons or non-U.S. persons located in the United States? May such foreign intelligence be collected

---

[11] The transcript of the interview with the DNI may be found at [http://www.elpasotimes.com/news/ci_6685679]. *See also*, "Greg Miller, Court Puts Limits on Surveillance Abroad: The ruling raises concerns that U.S. anti-terrorism efforts might be impaired at a time of heightened risk," *L.A. Times*, August 2, 2007, quoting a Member of Congress that "[t]here's been a ruling, over the last four or five months, that prohibits the ability of our intelligence services and our counterintelligence people from listening in to two terrorists in other parts of the world where the communication could come through the United States."

[12] For more information on the Protect America Act of 2007, see CRS Report RL34143, *P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act*, by Elizabeth B. Bazan (August 23, 2007).

[13] "United States person" is defined in section 101(I) of FISA to mean:

> a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), 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, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

from U.S. persons abroad without a Foreign Intelligence Surveillance Court[14] order pursuant to a certification by the Attorney General or the Attorney General and the DNI jointly or whether a court order is required prudentially or constitutionally under the Fourth Amendment.[15]

Generally, the full extent of Fourth Amendment protections attach to the privacy interests of U.S. persons within the United States. Fourth Amendment protections also attach to U.S. citizens abroad.[16] However, the operation of its protections outside the United States may differ from that in the United States due to the fact that a citizen abroad may not have the same expectation of privacy. In addition, the Warrant Clause of the Fourth Amendment may not apply outside the United States where U.S. magistrates have no jurisdiction.[17] A determination whether interception of a communication abroad is lawful turns upon the law of the country where the interception occurs, so, depending upon location, the rights available may differ significantly.[18] In addition, the availability of Fourth Amendment protections are affected by whom the search was executed, and the extent of any U.S. role, if any.[19] If the U.S. plays no role, then the Fourth Amendment does not attach, and the exclusionary rule does not apply to evidence obtained by or derived from such a

---

[14] As a general matter, the proposals contemplate that any such court order would be issued by the Foreign Intelligence Surveillance Court, created under section 103(a) of FISA, 50 U.S.C. § 1803(a).

[15] For a more in depth discussion of the application of the Fourth Amendment to U.S. citizens abroad, see CRS Congressional Distribution Memorandum entitled "U.S. Citizens' Fourth Amendment Rights Abroad and the Interception of Electronic Communications," by Jennifer K. Elsea (November 13, 2007).

[16] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990), suggests that the Fourth Amendment may have some applicability to aliens, such as permanent resident aliens, who have accepted societal obligations and made a significant voluntary commitment to the United States.

[17] United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (Kennedy, J., concurring)("The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment's warrant requirement should not apply in Mexico as it does in this country"); *id*. at 279 (Stevens, J., concurring in the judgment)("I do agree, however, with the Government's submission that the search conducted by the United States agents with the approval and cooperation of the Mexican authorities was not 'unreasonable' as that term is used in the first Clause of the Amendment. I do not believe the Warrant Clause has any application to searches of noncitizens' homes in foreign jurisdictions because American magistrates have no power to authorize such searches").

[18] Stowe v. Devoy, 588 F.2d 336, 342 (2d Cir. 1978); United States v. Cotroni, 527 F.2d 708, 711 (2d Cir. 1975).

[19] Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1969)("Neither the Fourth Amendment to the United States Constitution nor the exclusionary rule of evidence, designed to deter federal officers from violating the Fourth Amendment, is applicable to the acts of foreign officials").

search unless the foreign conduct "shocks the conscience."[20] On the other hand, if warrantless electronic surveillance targeted at a U.S. citizen's communications is conducted abroad for the purpose of gathering foreign intelligence by U.S. officials, the U.S. district court in *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), has held that it will be deemed reasonable if it is authorized by the President, or the Attorney General pursuant to the President's delegation, and the surveillance was conducted "primarily for foreign intelligence purposes and . . . targets foreign powers or their agents."[21]

In addition to considering the scope of constitutional privacy protections available to U.S. citizens or U.S. persons abroad, the 110th Congress, in FISA legislation before it, is also considering what it deems the appropriate level of privacy protection to be afforded such persons while outside the United States. In addition to the Protect America Act of 2007, P.L. 110-55 (August 5, 2007), noted above, differing views are reflected in H.R. 3773 as passed by the House of Representatives, S. 2248 as reported out of the Senate Select Committee on Intelligence, and S. 2248 as reported out of the Senate Judiciary Committee with an amendment in the nature of a substitute.[22]

H.R. 3773 provides that no court order is needed for electronic surveillance directed at acquisition of the contents of communications between persons not known to be U.S. persons who are reasonably believed to be located outside the United States, without regard to whether the communication is transmitted through the United States or the surveillance device is located in the United States. If the communications of a U.S. person are inadvertently intercepted, stringent constraints upon retention, disclosure, dissemination, or use would apply. However, the bill provides for a FISC order for acquisitions for up to one year of communications of non-U.S. persons reasonably believed to be outside the U.S. to collect most types of foreign intelligence information by targeting those persons, where those persons may be communicating with persons inside the United States. It also establishes requirements for such acquisitions. S. 2248 as reported out of the Senate Select Committee on Intelligence would permit the Attorney General and the DNI to jointly authorize, for up to one year, targeting of persons reasonably believed to be outside the U.S. to acquire foreign intelligence information if certain statutory criteria are met. The Senate Judiciary Committee's amendment in the nature of a substitute also

---

[20] United States v. Callaway, 446 F.2d 753, 755 (3d Cir. 1971); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976); Stowe v. Devoy, 588 F.2d 336, 341 (2d Cir. 1978); United States v. Rose, 570 F.2d 1358, 1362 (9th Cir. 1978); United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983); United States v. Delaplane, 778 F.2d 570, 573-74 (10th Cir. 1985); United States v. Rosenthal, 793 F.2d 1214, 1231-232 (11th Cir. 1986).

[21] *See* CRS Congressional Distribution Memorandum entitled "U.S. Citizens' Fourth Amendment Rights Abroad and the Interception of Electronic Communications," by Jennifer K. Elsea (November 13, 2007).

[22] *See, also,* H.R. 3782, H.R. 3321. For a side-by-side comparison of H.R. 3773 and the two reported versions of S. 2248, see CRS Report RL34277, *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*, by Elizabeth B. Bazan (December 6, 2007).

provides for the Attorney General and the DNI to jointly authorize targeting of persons reasonably believed to be outside the U.S. to acquire foreign intelligence information, but sets somewhat different criteria that must be satisfied.[23]

Limitations on Liability for Telecommunications Providers Furnishing Aid to the Government

The second of the two critical needs identified by the DNI in his August 2nd statement was a need for liability protection for those who furnish aid to the Government in carrying out its foreign intelligence collection efforts. He sought both retrospective relief from liability for those who are alleged to have aided the Government from September 11, 2001 to the present in connection with electronic surveillance or collection of other communications related information, and prospective liability protection for those telecommunications providers who furnish aid to the government in the future whether pursuant to a court order or a certification by the Attorney General or the Attorney General and the DNI that the acquisition or electronic surveillance involved is lawful and that all statutory requirements have been met.

Under current law, there are a number of statutory sections which provide some limitation on telecommunication providers who furnish aid to the government in connection with electronic surveillance or a physical search,[24] or the installation of a pen register or trap and trace device[25] pursuant to a court order under FISA. Section 105B(1) of FISA as added by the Protect America Act, P.L. 110-55, bars causes of action in any court against any person for providing any information, facilities, or assistance in accordance with a directive under that section. In addition, 18 U.S.C. § 2511(2)(a) bars suit in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or a certification in writing by the Attorney General or a person specified under 18 U.S.C. § 2518(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.[26]

Prospective relief from liability for those furnishing aid to the government pursuant to a court order or certification or a directive pursuant to statute requiring compliance with government demands for assistance is contemplated in a number of pending bills, including H.R. 3773, S. 2248 as reported out of the Senate Select Committee on Intelligence, and the Senate Judiciary Committee's amendment in the

---

[23] See CRS Report RL34277, *supra*, beginning at 3.

[24] 50 U.S.C. § 1805(I).

[25] 50 U.S.C. § 1842(f).

[26] *See also*, defenses against criminal liability in specified circumstances under 50 U.S.C. § 1809(b) (electronic surveillance) and 1827(b) (physical searches). *But see*, civil liability provisions under 50 U.S.C. §§ 1810 and 1828.

nature of a substitute to S. 2248.[27] Like P.L. 110-55, both versions of S. 2248 provide a means by which the person receiving such a directive may challenge its legality.[28] P.L. 110-55, H.R. 3773, and both versions of S. 2248 authorize the FISC to compel compliance through the contempt power.[29]

Retroactive immunity presents more difficult issues. There are currently pending a substantial number of law suits against the telecommunications providers who are alleged to have furnished aid to the government in connection with its warrantless surveillance programs since September 11, 2001, and other programs.[30] Approximately 40 of these suits are currently pending in the Northern District of California under an order of the Judicial Panel on Multidistrict Litigation. On August 9, 2006, pursuant to 28 U.S.C. § 1407, the Judicial Panel on Multidistrict Litigation transferred 17 civil actions that were pending throughout the country to the Northern District of California, and assigned them to Judge Vaughn Walker for coordinated or consolidated pretrial proceedings, In Re: National Security Agency Telecommunications Records Litigation, MDL-1791. Another 26 cases were treated as potential tag-along actions under the multidistrict litigation rules.(4) The panel of five federal trial and appellate court judges found that all these class actions share "factual and legal questions regarding alleged Government surveillance of telecommunications activity and the participation in (or cooperation with) that surveillance by individual telecommunications companies," and thus centralization of the cases "is necessary in order to eliminate duplicative discovery, prevent inconsistent pretrial rulings (particularly with respect to matters involving national security), and conserve the resources of the parties, their counsel and the judiciary."[31]

---

[27] *See* CRS Report RL34277, *supra*, at 19 for H.R. 3773; 17, 19, 49-54 (dealing with retroactive immunity), and 56 for S. 2248 as reported out of Senate Select Committee on Intelligence; and 17 and 19 for S. 2248 as reported out of Senate Judiciary Committee with an amendment in the nature of a substitute.

[28] *See* CRS Report RL34277, *supra*, at 15-17 for treatment of this issue by the two versions of S. 2248.

[29] *See* CRS Report RL34277, *supra*, at 19.

[30] *Cf*., CRS Report RL33424, *Government Access to Phone Calling Activity and Related Records: Legal Authorities*, by Elizabeth B. Bazan, Gina Marie Stevens, Brian T. Yeh (August 20, 2007). *Cf*., American Civil Liberties Union v. National Security Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2007), *vacated and remanded on other grounds*, 493 F.3d 644 (6th Cir. 2007). A petition for certiorari has been filed in the case on October 3, 2007. The district court, in pertinent part, held the plaintiffs' "datamining" claim barred by application of the state secrets privilege, 438 F. Supp. 2d at 759, 763, 782. This case was brought against government agencies and officers rather than against the telecommunications providers who may have assisted the government in its efforts.

[31] Transfer Order, MDL Docket No. 1791, In Re: National Security Agency Telecommunications Records Litigation. Other actions have been initiated against telecommunications providers by a public utility commission to seek information from or impose sanctions upon those providers. *See, e.g*., State of Maine Public Utilities Commission, Request for Commission Investigation into Whether Verizon is Cooperating in Maine with the National Security Agency's Warrantless Surveillance Program, Docket No.2006-274.

Neither H.R. 3773, nor the Senate Judiciary amendment in the nature of a substitute to S. 2248 address retrospective immunity. The Senate Select Committee on Intelligence's version of S. 2248, in title II, provides for retroactive immunity if certain criteria are met. S. 2042 takes a different approach. It would provide for substitution of the Government as the defending party for the telecommunications providers if statutory requirements were satisfied.

Arguments may be made on both sides with respect to whether retroactive immunity should be granted telecommunications providers who are alleged to have assisted the government in such programs. For example, the cooperation of such providers is critical to the government's capacity to pursue electronic surveillance to gather foreign intelligence information, and is also essential for collection of communications records for pattern analysis. If the telecommunication providers who responded to the government's requests or demands for assistance did so in good faith reliance upon assertions by the government that the demand was lawful and that a court order was not required, it may be argued that the providers should be immunized from ill effects flowing from such good faith reliance. Some have argued that the unique factual context militates in favor of such relief from liability, to the extent those who responded to the government's requests for assistance in the wake of 9/11 did so in response to government assertions that their cooperation was necessary to protect against further attacks.

In many of the suits filed, the government has asserted states secrets privilege with respect to the programs involved and the role of any of the telecommunications carriers with respect thereto. This is a common law evidentiary privilege, which may only be asserted by the government, that protects information from discovery when its disclosure would be inimical to the national security.[32] The privilege can come into play in three ways. If the very subject matter of the case is a state secret, an assertion of the privilege can cause the case to be immediately dismissed and the action barred. If, however, this prong of the state secrets privilege does not apply, the privilege may operate to bar admission into evidence of information which will damage the security of the United States. The plaintiff then goes forward on the basis of evidence not covered. If the plaintiff cannot prove a prima facie case with nonprivileged evidence, then the case may be dismissed.[33] On the other hand, if the privilege deprives a defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant.[34] In the current context, to the extent that a defendant telecommunications providers may have a valid claim of immunity under 18 U.S.C. § 2511(2)(a), but for the application of the state secrets privilege to the identities of

---

[32] In re United States, 8782 F.2d 472, 474-75 (D.C. Cir. 1989).

[33] This is the basis upon which the Sixth Circuit dismissed ACLU v. NSA, *supra*, on appeal, finding that the plaintiffs would be unable to demonstrate standing from nonprivileged evidence.

[34] *See*, Hepting v. AT&T, 439 F. Supp. 2d 974, 984 (N.D. Cal. 2006), *citing* Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998). The *Hepting* court held that the case was not barred on the basis that its very nature was a state secret, but that there was insufficient information to determine whether the other two prongs applied. The other consolidated cases have been stayed pending the interlocutory appeal of the *Hepting* decision.

any providers who may have furnished aid to the government, an argument may be made that the telecommunications providers so impacted should be afforded immunity from suit.

On the other hand, such suits may be the only means by which those who may have been adversely impacted by such government activities may obtain any remedy for any injuries incurred. These injuries may have impacted First and Fourth Amendment protected interests, and there may be no other means of vindicating those rights. In addition, the telecommunications providers provide the front line of defense of those rights against governmental abuse if the government demand or request is unlawful. In some instances, it may be argued that a telecommunications provider has a statutory obligation to protect customer records from unlawful access.[35] Such arguments militate against affording relief from liability to any providers who may have permitted unlawful access.

In addition to these arguments, some have argued that, because the Administration has not shared information repeatedly sought by some committees of jurisdiction with respect to the role of the telecommunications providers in the TSP or other pertinent intelligence activities, the Congress does not have adequate information to determine whether relief for the telecommunications carriers is warranted.

[35] See, e.g., 47 U.S.C. § 222 (protection of customer proprietary network information.)