

# CRS Report for Congress

## The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues

July 7, 2008

Elizabeth B. Bazan  
Legislative Attorney  
American Law Division



Prepared for Members and  
Committees of Congress

# The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues

## Summary

The current legislative and oversight activity with respect to electronic surveillance under the 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 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 or from United States persons abroad, 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. This report briefly examines these issues and sets them in context.

The 110<sup>th</sup> Congress has been very active in developing and considering measures to amend FISA to address these issues. On August 5, 2007, the Protect America Act, P.L. 110-55, was enacted into law. It expired on February 16, 2008, after passage of a fifteen-day extension to its original sunset date. *See* P.L. 110-182. On November 15, 2007, the House of Representatives passed H.R. 3773, the RESTORE Act of 2007. On February 12, 2008, the Senate passed S. 2248, as amended, then struck all but the enacting clause of H.R. 3773, and inserted the text of S. 2248, as amended, in its stead. On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773. After months of intensive negotiations, on June 19, 2008, a compromise bill, H.R. 6304, was introduced in the House. It was passed by the House the following day. On June 26, 2008, a cloture motion on the measure was presented in the Senate. Further activity on H.R. 6304 is anticipated after the Senate returns from the July 4<sup>th</sup> recess. Each of these bills differ somewhat in content and approach from one another.

This report consists of the text of CRS Report RL34279, *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, by Elizabeth B. Bazan, without the accompanying footnotes. It will be updated as needed.

## Contents

Introduction .....	1
Tension Between National Security and Civil Liberties .....	2
Collection of Foreign Intelligence Information from Foreign Persons and United States Persons Located Abroad .....	4
Legislative Response: Foreign Intelligence Surveillance of Foreign Persons Abroad .....	6
Legislative Response: Foreign Intelligence Surveillance of U.S. Persons Outside the United States .....	8
Limitations on Liability for Telecommunications Providers Furnishing Aid to the Government .....	9
Legislative Response .....	11

# The Foreign Intelligence Surveillance Act: A Sketch of Selected Issues

## Introduction

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. While FISA now provides 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 110<sup>th</sup> Congress. On August 5, 2007, the Protect America Act, P.L. 110-55 was enacted into law. This measure, in part, construed the term “electronic surveillance” under FISA not to include surveillance directed at a person reasonably believed to be located outside of the United States, and provided authority for warrantless acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States where certain criteria were satisfied. As originally enacted, the measure was to sunset on February 1, 2008. On January 29, 2008, both the House and the Senate passed H.R. 5104, a 15-day extension to the sunset for the Protect America Act, to allow further time to consider, pass, and go to conference on proposed legislation to amend FISA, while ensuring that the intelligence community would have the authority it needed in the intervening period. It was enacted into law as P.L. 110-182.

The House of Representatives passed H.R. 3773, the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007 or the RESTORE Act of 2007 on November 15, 2007, while S. 2248 was reported out of the Senate Select Committee on Intelligence on October 26, 2007, and an amendment in the nature of a substitute to S. 2248, the Foreign Intelligence Surveillance Amendments Act of 2007 or the FISA Amendments Act of 2007, was reported out

of the Senate Judiciary Committee on November 16, 2007. A modified version of the Senate Judiciary Committee's amendment in the nature of a substitute to S. 2248 was tabled.

The Senate passed S. 2248, the FISA Amendments Act of 2008, as amended, on February 12, 2008. After striking all but the enacting clause of H.R. 3773 and inserting the text of S. 2248 as amended, the Senate then passed H.R. 3773, the FISA Amendments Act of 2008.

On March 14, 2008, the House passed an amendment to the Senate amendment to H.R. 3773. After intensive negotiations, a compromise bill, H.R. 6304, was introduced in the House on June 19, 2008. The measure passed the House the following day. A cloture motion on the measure was presented in the Senate on June 26, 2008. Further activity on H.R. 6304 is anticipated after the Senate returns from the July 4<sup>th</sup> recess.

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 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. This report briefly examines 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.

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.

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. . . .

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.

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.

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. 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 Qaeda 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.” 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 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 and United States 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 and United States 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.

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 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.

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

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, 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 from U.S. persons abroad without a Foreign Intelligence Surveillance Court 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?

## **Legislative Response: Foreign Intelligence Surveillance of Foreign Persons Abroad**

On August 5, 2007, the Protect America Act of 2007 was enacted into law, 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. This authority was similar, but not identical to, the proposed section 102A of FISA in the Administration’s draft bill. P.L. 110-55 expired on February 16, 2008, after passage of a fifteen-day extension to its original sunset date. Under the transitional provisions in Section 6 of the Protect America Act, the acquisitions authorized while the act was in force may continue until their expiration.

H.R. 3773 as originally passed by the House 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.

The Senate amendment to H.R. 3773 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 bill does not require prior approval by the FISC of applicable certifications, targeting procedures and minimization procedures in connection with the acquisition of communications of non-U.S. persons abroad, nor does it require adoption and submission of compliance guidelines. Rather, it requires submission of a certification or a targeting or minimization procedure, or an amendment thereto, to the Foreign Intelligence Surveillance Court (FISC) within five days of making or amending the certification or adopting or amending the procedure. Where the Attorney General and the DNI determine that immediate action is required and time does not permit preparation of a certification prior to initiation of an acquisition, the Senate bill requires the Attorney General and the DNI to prepare the certification, including such determination, within seven days after the determination is made. If the FISC finds that a certification meets statutory requirements and targeting and minimization procedures are consistent with statutory requirements and meet constitutional standards under the Fourth Amendment, the FISC would enter an order approving continued use of the procedures involved. If the court finds that the required standards are not met, then the FISC would enter an order directing the government, at the government's election and to the extent required by the FISC order, to correct any deficiencies within 30 days or cease the acquisition.

In the absence of an emergency authorization, the House amendment to the Senate amendment to H.R. 3773 requires prior approval by the FISC of the applicable targeting procedures, minimization procedures, and certification before the Attorney General and the Director of National Intelligence (DNI) may authorize acquisition of the contents of communications of non-U.S. persons reasonably believed to be located outside the United States. The FISC would have 30 days after a certification is submitted to review the certification and the targeting and minimization procedures and to approve or deny an order regarding such an acquisition.

The House amendment also requires the Attorney General, in consultation with the DNI, to adopt guidelines to ensure compliance with limitations imposed by the bill on such acquisitions and to ensure that an application is filed under section 104 or 303 of FISA, if required by that act. The guidelines are to be submitted to the FISC, the congressional intelligence committees, and the House and Senate Judiciary Committees.

H.R. 6304 would amend FISA to permit the Attorney General and the DNI to jointly authorize targeting of persons reasonably believed to be non-U.S. persons located outside the United States for periods of up to one year. Proposed section 702 of FISA contains explicit limitations, including protections against reverse targeting in connection with the acquisition of the communications of such persons. A certification by the Attorney General and the DNI that certain statutory criteria have been met, applicable targeting procedures, and minimization procedures would be

subject to judicial review by the FISC. The certification would attest, in part, that procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States. Generally, if the certification and targeting and minimization procedures meet the statutory requirements and are consistent with the Fourth Amendment, a FISC order approving them would be issued prior to implementation of the acquisition of the communications at issue. If the FISC finds deficiencies in the certification, targeting procedures, or minimization procedures, the court would issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any such deficiency within 30 days or cease, or not begin, the implementation of the authorization for which the certification was submitted.

## **Legislative Response: Foreign Intelligence Surveillance of U.S. Persons Outside the United States**

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. 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. 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. 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 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 search unless the foreign conduct "shocks the conscience." 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."

In addition to considering the scope of constitutional privacy protections available to U.S. citizens or U.S. persons abroad, the 110<sup>th</sup> 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), the Senate-passed amendment to H.R. 3773, the House-passed amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each addresses procedures for targeting U.S. persons

reasonably believed to be located outside the United States to collect foreign intelligence information.

The Senate amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304 each provide for targeting of U.S. persons reasonably believed to be located outside the United States for up to 90 days pursuant to a FISC order if statutory criteria are met. Such an order could be renewed for additional 90-day periods upon submission of renewal applications meeting the same standards. In the case of an emergency authorization by the Attorney General of an acquisition, each bill requires notice to a FISC judge by the Attorney General or his designee at the time the decision is made to conduct such an acquisition and requires the filing of an application for a FISC order within seven days of the Attorney General's authorization of the emergency acquisition. Minimization procedures would apply to such an acquisition.

Under each of these bills, in the absence of a judicial order approving an acquisition originally authorized by the Attorney General on an emergency basis, the acquisition would terminate when the information sought is obtained, when an application for the order is denied, or when seven days have elapsed, whichever is earliest. Without a FISC order, no information acquired or evidence derived from an emergency acquisition, except under circumstances where the target of the acquisition is determined not to be a U.S. person, may be received in evidence or disclosed in federal, state, or local proceedings; nor could any information concerning a U.S. person acquired from such acquisition subsequently be used or disclosed in any other manner by federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

## **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 2<sup>nd</sup> 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 liability for telecommunication providers who furnish aid to the government in connection with electronic surveillance or a physical search, or the installation of a pen register or trap and trace device pursuant to a court order under

FISA. 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.

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 bills, including H.R. 3773 as originally passed, the Senate Amendment to H.R. 3773, the House amendment to the Senate amendment to H.R. 3773, and H.R. 6304. All three versions of H.R. 3773, and H.R. 6304 authorize the FISC to compel compliance through the contempt power, as did P.L. 110-55 while it was in force.

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. 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 *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. 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.”

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 state 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. 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. 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. 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 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. 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.

## **Legislative Response**

Under proposed section 802(a) of FISA in Title II of H.R. 6304, a civil action may not lie or be maintained in a federal or state court against any person for providing assistance to an element of the intelligence community, and must be dismissed promptly, if the Attorney General certifies to the U.S. district court in which the action is pending that:

- (1) any assistance by that person was provided pursuant to an order of the court established under section 103(a) directing such assistance;

- (2) any assistance by that person was provided pursuant to a certification in writing under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, United States Code;
- (3) any assistance by that person was provided pursuant to a directive under section 102(a)(4), 105B(e), as added by section 2 of the Protect America Act of 2007 (Public Law 110-55), or 702(h) directing such assistance;
- (4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was —
  - (A) in connection with an intelligence activity involving communications that was —
    - (i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
    - (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and
  - (B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was —
    - (i) authorized by the President; and
    - (ii) determined to be lawful; or
- (5) the person did not provide the alleged assistance.

Under proposed subsection 802(b) of FISA, such a certification shall be given effect unless the court finds that it is not supported by substantial evidence provided to the court under that section. In the course of its judicial review, the U.S. district court may examine the court order, certification, written request, or directive described in proposed subsection 802(a) and any relevant court order, certification, written request, or directive submitted to the court by the parties under proposed subsection 802(d). Any such party would be permitted to participate in briefing or argument of any legal issue in a judicial proceeding under this section to the extent that such participation does not require disclosure of classified information to that party. Any relevant classified information would be reviewed in camera and ex parte. Any portion of the court's written order that would reveal classified information would be issued in camera and ex parte and maintain it under seal. Upon filing of a declaration by the Attorney General under 28 U.S.C. § 1746 that disclosure of such a certification or of the supplemental materials provided pursuant to proposed subsections 802 (b) or (d) would harm the national security of the United States, the U.S. district court would be required to review such certification and the supplemental materials in camera and ex parte. Any public disclosure of such certification and supplemental materials would be limited to a statement as to whether the case is dismissed and a description of the legal standards that govern the order, without disclosing the paragraph of subsection (a) that is the basis for the certification. If H.R. 6304 were to be enacted into law, proposed Section 802 of FISA would apply to a civil action pending on or filed after the date of the enactment.

The Senate amendment to H.R. 3773 bars covered civil actions in a federal or state court and requires that such an action must be dismissed promptly if the Attorney General or above certifies to the court that the assistance alleged to have been provided by the electronic communication service provider was 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; and designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was authorized by the President and determined to be lawful. A covered civil action in federal or state court would also be barred and should be dismissed promptly if the Attorney General certifies to the court that the electronic communication service provider did not provide the alleged assistance. The Attorney General's certification would be subject to judicial review under an abuse of discretion standard. If the Attorney General files a declaration under 28 U.S.C. § 1746 that disclosure of a certification made under subsection 202(a) of the bill would harm United States national security, the court shall review the certification in camera and ex parte, and limit public disclosure concerning such certification, including any public order following such ex parte review, to a statement that the conditions of subsection 202(a) of the bill have been met, without disclosing the subparagraph of subsection 202(a)(1) that is the basis for the certification. The authorities of the Attorney General under section 202 are to be performed by the Attorney General, or the Acting Attorney General, or a designee in a position not lower than the Deputy Attorney General.

The House-passed amendment to the Senate Amendment took a different approach. Proposed section 802, in part, provides authority for the government to intervene in any covered civil action. Any party may submit to the court evidence, briefs, arguments, or other information on any matter with respect to which a state secrets privilege has been asserted. The section also authorizes the court to review any such submissions in accordance with procedures set forth in section 106(f) of FISA; and permits the court, on motion of the Attorney General, to take additional steps to protect classified information. The court, to the extent practicable and consistent with national security would be permitted to request any party to present briefs and arguments on any legal question the court finds raised by such submission, regardless of whether that party has access to the submission. Under new subsection 802(e) of FISA, for any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the period from September 11, 2001 through January 17, 2007, the Attorney General would be required to provide to the court any request or directive related to the allegations under the procedures set forth in new subsection 802(b).

H.R. 6304, therefore, differs from prior House and Senate amendments to H.R. 3773 in a number of respects, while having similarities to them in others. Both H.R. 6304 and the Senate amendment would bar civil actions in federal or state court against persons providing assistance to an element of the intelligence community if the Attorney General certifies that certain statutory criteria are met. They differ to some degree as to the criteria involved.

H.R. 6304 provides for judicial review of the Attorney General's certification under a substantial evidence standard, while the Senate amendment to H.R. 3773 provides for review of the Attorney General's certification using an abuse of discretion standard. The House amendment to the Senate amendment to H.R. 3773 provides for judicial review of any submissions by any party relating any matter as



to which state secrets privilege has been asserted, but does not specify the standard of review.

H.R. 6304 expressly permits the district court, in its review, to examine any court order, certification, written request, or directive described in proposed subsection 802(a) or submitted to the court by the parties, and, permits party participation in briefs and arguments on any legal issue in the judicial proceeding to the extent that such participation does not require disclosure of classified information to that party. This does not have a parallel in the Senate amendment. However, it has some points of similarity with the House amendment, which permits submissions by the parties of evidence, briefs, arguments, or other information relating to any matter with respect to which state secrets privilege has been asserted, while providing protections for classified information. For any covered civil action alleging that a person provided assistance to an element of the intelligence community pursuant to a request or directive during the September 11, 2001 to January 17, 2007 period, the House amendment requires the Attorney General to provide the court with any request or directive related to the allegations.

All three bills make provision for ex parte, in camera review of classified information. H.R. 6304 and the Senate amendment both place restrictions on public disclosure of information regarding the certification and the court's order.