Order Code RL34600

CRS Report for Congress

Retroactive Immunity Provided by the FISA Amendments Act of 2008

July 25, 2008

Edward C. Liu
Legislative Attorney
American Law Division

Prepared for Members and Committees of Congress

Retroactive Immunity Provided by the FISA Amendments Act of 2008

Summary

On July 10, 2008, P.L. 110-261, entitled the FISA Amendments Act of 2008, was signed into law. Although many of the changes enacted by the FISA Amendments Act were controversial, one particularly contentious issue was whether to grant retroactive immunity to telecommunications providers that may have facilitated warrantless surveillance by the federal government under a Terrorist Surveillance Program between 2001 and 2007. Proponents of retroactive immunity argued that it was necessary to assure private cooperation with critical intelligence investigations. On the other hand, opponents of retroactive immunity argued that its inclusion undermined the statutory penalties that were designed to deter unlawful intrusions into individual liberties. This report discusses the various retroactive immunity mechanisms that were proposed to be included in the FISA Amendments Act, one of which was ultimately adopted, and their likely effect on lawsuits facing telecommunications providers.

Retroactive immunity is more than simply protection from liability; it can also act as protection from the cost of litigation. Without retroactive immunity, many legal issues would need to be addressed, possibly at great expense, in order to resolve these lawsuits. The plaintiffs would need to show that the actions of the defendants were not lawful. The Bush Administration's theory of inherent wiretapping ability might need to be litigated. Additionally, the applicability of the state secrets privilege to these cases might be the subject of litigation.

As enacted, the FISA Amendments Act lays out a procedure for the Attorney General to bring about the dismissal of lawsuits alleging unlawful participation in the Terrorist Surveillance Program (TSP). In order for a suit to be dismissed by a court, the Attorney General must certify that the defendant provided assistance in connection with the TSP and was given written assurances that the program was authorized by the President and determined to be lawful. The Attorney General could also certify that the alleged assistance was not in fact provided by the defendant. All parties are permitted to submit documents and arguments relevant to dismissal which the court may consider. Dismissal is only proper if the court finds, based upon its review, that the Attorney General's certification is supported by "substantial evidence."

Contents

Retroactive Immunity Provided by the FISA Amendments Act of 2008

In November of 2007, the House of Representatives passed H.R. 3773, the RESTORE Act, which would have amended several provisions of the Foreign Intelligence Surveillance Act (FISA). In February of 2008, the Senate passed an amendment in the nature of a substitute to H.R. 3773. The Senate amendment included, among other things, a provision allowing the Attorney General to seek the dismissal of civil lawsuits brought by private citizens against telecommunications providers that may have assisted the federal government in carrying out warrantless electronic surveillance. In March of 2008, the House responded by passing a third version of H.R. 3773 removing the retroactive immunity provisions, but later passed a compromise bill, H.R. 6304, in June. H.R. 6304 included a variation on the retroactive immunity provisions of the Senate's version of H.R. 3773. In July of 2008, the Senate passed H.R. 6304, also titled the FISA Amendments Act of 2008 (FISA Amendments Act), without modification, and the President subsequently signed it into law.[1] This report discusses the effect of the retroactive immunity provided by the FISA Amendments Act on lawsuits alleging unlawful electronic surveillance by telecommunications providers under a Terrorist Surveillance Program (TSP) between 2001 and 2007.

The Terrorist Surveillance Program

In late 2005, the *New York Times* reported that the federal government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[2] Subsequently, President Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National Security Agency to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations" based upon "his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy."[3] The revelation of the existence of the TSP aroused controversy because it appeared to run afoul of the general rule[4] that electronic surveillance by the federal government is unlawful unless

---

[1] FISA Amendments Act of 2008, P.L. 110-261 (July 10, 2008).

[2] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NEW YORK TIMES, Dec. 16, 2005, at 1.

[3] U.S. DEP'T OF JUSTICE, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, at 5, 17, Jan. 19, 2006, available at [http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf].

[4] The "procedures in [Title III of the Omnibus Crime Control and Safe Streets Act] and the (continued...)

conducted pursuant to the Foreign Intelligence Surveillance Act (FISA)[5] or Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[6] In contrast, the Bush Administration's position has been that such warrantless surveillance is lawful under the President's constitutionally granted authority and the Authorization for Use of Military Force (AUMF) enacted by Congress in 2001.[7]

On Jan 17, 2007, a letter from the Attorney General to Congress indicated that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program [would] be conducted subject to the approval of the Foreign Intelligence Surveillance Court." Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to sometime in January of 2007.[8]

Dozens of lawsuits have been filed by private citizens and interest groups alleging various statutory and constitutional violations by the telecommunications companies that participated in the TSP.[9] The debate over retroactive immunity is of central importance to these cases, as it would likely render any litigation of the underlying legal issues moot.[10] On August 2, 2007, the Director of National Intelligence (DNI) stated that "those who assist the Government in protecting us from harm must be protected from liability," specifically "those who are alleged to have assisted the Government after September 11, 2001 and have helped keep the country safe."[11] Proponents of retroactive immunity also argued that without "the [telecommunications providers'] voluntary cooperation it [foreign intelligence gathering] is much harder and we get much less [information]."[12] On the other hand, opponents of retroactive immunity pointed out that retroactive immunity "strips [unlawfully surveilled] individuals of the ability to vindicate their rights in court

---

[4] (...continued)
Foreign Intelligence Surveillance Act of 1978 shall be *the exclusive means* by which electronic surveillance, as defined in section 101 of FISA, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

[5] P.L. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801 *et seq.*).

[6] P.L. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*).

[7] P.L. 107-40, 115 Stat. 224 (2001). *See, also,* CRS Congressional Distribution Memo, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information,* by Elizabeth B. Bazan and Jennifer K. Elsea (Jan. 5, 2008).

[8] S.Rept. 110-209, at 4.

[9] *Id.* at 7.

[10] For a more detailed discussion of these lawsuits and retroactive immunity, *see*, CRS Report RL34279, *The Foreign Intelligence Surveillance Act: An Overview of Selected Issues*, by Elizabeth B. Bazan, at 14-21.

[11] Admiral Michael McConnell, Director of Nat'l Intelligence, *Modernization of the Foreign Intelligence Surveillance Act (FISA),* Aug. 2, 2007, available at [http://www.odni.gov/press_releases/20070802_release.pdf].

[12] 154 CONG. REC. S6454 (daily ed. July 9, 2008) (statement of Sen. Bond).

regarding wiretapping abuses of the past,"[13] and that "if we want [telecommunications providers] to follow the law in the future, it sends a terrible message, and sets a terrible precedent, to give them a 'get out of jail free' card for allegedly ignoring the law in the past."[14]

Issues Raised by Civil Actions Against Telecommunications Providers

Retroactive immunity is more than simply protection from liability; it can also act as protection from the cost of litigation. Therefore, before discussing the effects of any retroactive immunity provisions, it may be helpful to examine how a covered lawsuit might proceed in the absence of retroactive immunity. Without retroactive immunity, many legal issues would need to be addressed, possibly at great expense, in order to resolve these cases. The plaintiffs would need to show that the actions of the defendants were not lawful under the laws in effect when the TSP was active. The Bush Administration's theory of inherent wiretapping ability might be litigated. Additionally, the applicability of the state secrets privilege could also be the subject of litigation. Each of these issues is discussed below.

Lawfulness Under the FISA and Title III

As a general principle, if electronic surveillance is likely to result in the acquisition of communications to or from someone in the United States such surveillance may not be conducted unless sanctioned by a court order.[15] Federal law provides two statutory frameworks for obtaining warrants to conduct electronic surveillance: Title III of the Omnibus Crime Control and Safe Streets Act and FISA. Title III authorizes electronic surveillance in the context of law enforcement, while FISA authorizes electronic surveillance in the context of gathering foreign intelligence. Both Title III and FISA also provide prospective civil immunity for individuals that assist or conduct electronic surveillance under the auspices of either statutory framework.[16]

---

[13] ACLU, *Letter to the Senate Urging No Votes On Any Bill That Would Authorize Warrantless Wiretapping or Grant Immunity to Telecoms*, Feb. 2, 2008, available at [http://www.aclu.org/safefree/general/33909leg20080204.html].

[14] 154 CONG. REC. S6381 (daily ed. July 8, 2008) (statement of Sen. Feingold).

[15] *But*, 50 U.S.C. § 1802 authorizes electronic surveillance without a court order for up to one year, *if* the targets are means of communications, property, or premises used exclusively by foreign governments, *and* there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party. Exceptions also apply during emergency situations or after congressional declarations of war. *Infra*, note 19. For a thorough description and analysis of federal wiretapping laws, *see*, CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle.

[16] 18 U.S.C. § 2511(2)(a)(ii) bars civil actions against telecommunications providers that give assistance pursuant to a court order or certification issued under Title III. FISA bars (continued...)

Plaintiffs suing telecommunications providers, and others, argue that the TSP was not lawful under either Title III or FISA. Many of the details of the TSP remain classified, but it apparently authorized the surveillance of international communications without a judicially issued warrant if there was a "reasonable basis to conclude that one party to the conversation [was] a member of al Qaeda."[17] That determination appears to have been made by intelligence officials, and was reported to have been reviewed every 45 days.[18] In contrast, Title III and FISA only allow *warrantless* surveillance for shorter periods of time in most circumstances.[19] Statements by officials in the Bush Administration appear to acknowledge that the TSP was conceived and operated outside of the procedures authorized by either Title III or FISA.[20]

Executive Authority and the Authorization for Use of Military Force

Nonetheless, the Bush Administration has argued, in support of the TSP, that the Constitution grants the executive the inherent power to conduct electronic surveillance to gather foreign intelligence and the AUMF reflects a congressional

---

[16] (...continued)
civil actions against the same type of defendants for assistance given pursuant to surveillance authorized by that statute. 50 U.S.C. § 1805(h).

[17] Press Briefing, *infra* note 20.

[18] President George W. Bush, Press Conference, Dec. 19, 2005, available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html].

[19] *See*, 18 U.S.C. § 2518(7) (authorizing warrantless electronic surveillance for 48 hours in situations involving immediate danger to persons, threats to national security, or organized crime); 50 U.S.C. § 1805(e) (authorizing emergency warrantless electronic surveillance for up to 72 hours while a court order is sought); and 50 U.S.C. § 1811 (authorizing warrantless electronic surveillance for 15 days following a Congressional declaration of war). *But*, *see*, discussion of authority to conduct warrantless electronic surveillance for up to one year, *supra*, note 15.

[20] For example, Attorney General Alberto Gonzales made the following statement:

> [FISA] is a very important tool that we continue to utilize. Our position is that we are not legally required to do [sic], in this particular case, because the law requires that we — FISA requires that we get a court order, unless authorized by a statute, and we believe that authorization has occurred.

General Michael Hayden, Principal Deputy Director for National Intelligence, elaborated further on that statement:

> [B]ecause of the speed, because of the procedures, because of the processes and requirements set up in the FISA process, I can say unequivocally that we have used this program [the TSP] in lieu of that [FISA] and this program has been successful.

Attorney General Alberto Gonzales and General Michael Hayden, Press Briefing, Dec. 19, 2005, available at [http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html].

intent to give the executive the authority to take all measures necessary to combat terrorism. A full exposition of the support for these propositions is beyond the scope of this report.[21] However, one should note that the question would require reconciling the assertions of the Bush Administration with the legislative history and statutory text of FISA and Title III which identify those statutes as the exclusive means of conducting electronic surveillance.[22] Here, it is sufficient to note that it is an issue that would likely require extensive litigation in order to be resolved.

The State Secrets Privilege

In some cases, the confidential subject matter of a suit may prevent a court from hearing it. Under the judicially created state secrets privilege, "public policy forbids the maintenance of any suit ... the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential."[23] Insofar as many of the details of the TSP remain classified, it is likely that the state secrets privilege would be central to the disposition of the suits against telecommunications providers discussed above.

The state secrets privilege is held by the government, meaning that only the government can assert it to preclude litigation.[24] If claimed by the federal government, the effect of the state secrets privilege can range from the exclusion of certain information from discovery or admission at trial to the complete dismissal of a civil action.[25] For example, in *Totten v. United States*, a former spy brought suit to enforce a secret contract with the federal government for espionage services. Ultimately, in that case, the Supreme Court held that the subject of litigation, namely the contract for espionage, was itself a secret and any litigation on that subject was barred.[26]

In other circumstances, the state secrets privilege applies only to certain items of evidence, rather than to the subject of litigation at large. In *Halkin v. Helms*, the D.C. Circuit was confronted with a claim of privilege regarding the NSA's alleged interception of international communications to and from persons who had been targeted by the CIA.[27] After deciding that the claim of privilege was valid, the court of appeals affirmed the protection of *that* information from discovery, while

---

[21] For a detailed analysis of the Bush Administration's arguments, s*ee*, CRS Congressional Distribution Memo, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea (Jan. 5, 2008).

[22] *Id.* at 40-41.

[23] *Totten v. United States*, 92 U.S. 105, 107 (1876) (applying the privilege to bar a suit to enforce a secret contract for espionage).

[24] *United States v. Reynolds*, 345 U.S. 1, 7 (1953).

[25] *See, Id.* at 11 n.26 (quoted by *Hepting v. AT&T*, 439 F. Supp. 2d 974, 984 (N.D. Cal. 2006)).

[26] *Totten*, 92 U.S. at 107.

[27] *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982).

permitting *other* evidence that the plaintiffs were targeted by the CIA.[28] In the end, however, the court dismissed the suit after deciding that without the privileged information, the plaintiffs would not be able to make a *prima facie* case.

A similar result may occur if the state secrets privilege requires the exclusion of evidence central to a defendant's case. In *Molerio v. Federal Bureau of Investigation*, a job seeker alleged that the FBI had disqualified him based upon his father's political ties to socialist organizations in violation of his father's First Amendment rights.[29] In response, the FBI asserted that it had a lawful reason to disqualify the plaintiff, but claimed that its reason was protected by the state secrets privilege. After reviewing the FBI's claim *in camera*, the D.C. Circuit agreed that the evidence of a nondiscriminatory reason was protected and that its exclusion would deprive the FBI of a valid defense. Therefore, the dismissal of that action was required.[30]

Although it is not possible to accurately determine whether the state secrets privilege would necessitate dismissal of the telecommunications cases discussed above, several courts presented with lawsuits regarding the TSP have issued preliminary rulings regarding the applicability of the state secrets privilege.

In *Hepting v. AT&T*, the district court was presented with an assertion of the state secrets privilege.[31] The court first examined whether the information requested was actually secret, given the amount of media publicity regarding the TSP and public statements made by the Bush Administration and the defendant.[32] While the *specifics* of the TSP may remain classified, the court noted that the general subject of the litigation, specifically that such a program existed at all, was no longer a secret given the admissions made by the government and the defendant. Therefore, this case was distinguishable from *Totten*, and dismissal of the case at the outset of litigation was inappropriate.[33] While the privilege may limit the plaintiffs' discovery efforts or the defendant's assertion of a defense at a later date, the court declined to rule on whether that would ultimately necessitate dismissal.[34]

FISA may preempt the state secrets privilege. In *In re National Security Agency Telecommunications Records Litigation*, the court considered 50 U.S.C. § 1806(f), which mandates a legislatively created procedure for courts to consider sensitive material, the disclosure of which might damage the national security of the United

---

[28] The other evidence of CIA targeting was never claimed to be privileged by the government. *Id.* at 997.

[29] *Molerio v. FBI*, 749 F. 2d 815, 824-825 (D.C. Cir. 1984).

[30] *Id.* at 825.

[31] *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006).

[32] *Id.* at 986.

[33] *Id.* at 993.

[34] *Id.* at 994.

States.[35] Section 1806(f), which was left unmodified by the FISA Amendments Act, requires sensitive information to be reviewed by courts *ex parte* and *in camera* with adequate procedures to safeguard against inadvertent disclosure.[36] The court found that this legislative framework trumped the judicially created state secrets privilege, despite arguments that the privilege was of constitutional origin.[37] The court did not preclude assertion of the privilege where FISA did not apply.[38] In the case before it, the plaintiffs had yet to show standing as "aggrieved persons" under FISA. Therefore, the court continued to bar the privileged information, but only until the plaintiffs had the opportunity to show, through other evidence, whether they are "aggrieved persons."[39]

Retroactive Immunity Under the FISA Amendments Act of 2008

Title II of the FISA Amendments Act lays out a procedure for the Attorney General to seek the dismissal of lawsuits alleging unlawful participation in the TSP by telecommunications providers. The process begins when the Attorney General certifies, to the court where the lawsuit is pending, two fundamental facts regarding the defendant's alleged assistance. First, the assistance must have been given in connection with the TSP between September 11, 2001, and January 17, 2007. Second, the defendant must have been given written assurances that the TSP was authorized by the President and determined to be lawful. Alternatively, the Attorney General can certify that the alleged assistance was not in fact provided by the defendant. All parties are permitted to submit documents and arguments which the court may consider, and dismissal is required if the court finds, based upon its review, that the certification was supported by "substantial evidence." What constitutes substantial evidence is discussed in the section below regarding standards of review.

Alternative Retroactive Immunity Proposals

Before the passage of H.R. 6304 by the Senate, that body had previously included retroactive immunity for telecommunications providers in its amendment to H.R. 3773. Additionally, three amendments were proposed to H.R. 6304 that would have modified the retroactive immunity provisions. This section examines the

---

[35] *See, In re National Security Agency Telecommunications Records Litigation*, No. 06-1791 VRW, slip op. at 18 (N.D. Cal. July 2, 2008) (holding that FISA's procedures for a court's *in camera* review of classified information preempts the common law state secrets privilege).

[36] 50 U.S.C. § 1806(f)

[37] *In re National Security Agency Telecommunications Records Litigation, supra*, note 35, at 20-22.

[38] *Id.* at 17.

[39] *Id.* at 48-49. *See,* 50 U.S.C. § 1801(k) (defining "aggrieved persons").

different approaches to retroactive immunity in that bill and the proposed amendments.

Senate Amendment to H.R. 3773

In February of 2008, the Senate passed an amendment in the nature of a substitute to H.R. 3773. Like H.R. 6304, this Senate amendment would have required courts to dismiss lawsuits against telecommunications providers if sufficient grounds for dismissal were certified to the court by the Attorney General.[40] With respect to the lawsuits alleging assistance provided under the TSP, the grounds for dismissal were identical to those required under H.R. 6304. But, H.R. 3773 did not provide a means for others to submit arguments or documents in opposition to dismissal, and certifications would only be subject to review for an abuse of discretion.[41] What qualifies as an abuse of discretion is discussed in the section below regarding standards of review.

Proposed Amendments to H.R. 6304

Three amendments offering variations on the retroactive immunity mechanism were introduced in the Senate during the debate over H.R. 6304, but were not adopted.

S.Amdt. 5059. Introduced by Senator Specter, S.Amdt. 5059 would have added a second component to a court's review of a certification by the Attorney General. Under this amendment, dismissal would not be appropriate if the court determined that the underlying intelligence activity that the defendant had participated in was unconstitutional. Because this would have been a legal determination, the court would have been permitted to address this question *de novo* without relying upon or giving deference to any interpretations of the Constitution made by the Attorney General in the certification or elsewhere.

S.Amdt. 5060. Introduced by Senator Whitehouse, S.Amdt. 5060 would have required that the Attorney General additionally certify that the defendant had provided assistance based on a "good faith and reasonable belief" that its conduct was lawful. Like the rest of the certification, this finding would have needed to be supported by "substantial evidence" in order to result in a dismissal.

S.Amdt. 5066. Introduced by Senator Bingaman, S.Amdt. 5066 would have left the certification mechanism of H.R. 6304 in place, but would have delayed certification by the Attorney General in cases involving the TSP until 90 days after the inspectors general of various intelligence and national security agencies had reviewed the TSP and submitted a comprehensive report to Congress detailing their findings. Additionally, all TSP lawsuits would have been stayed during this time. The review and report are still mandated by a separate provision of H.R. 6304, § 301,

---

[40] H.R. 6304, § 201, 110th Cong.

[41] H.R. 3773, § 202(a) as amended by the Senate, 110th Cong.

and are required to be completed within one year of the date of enactment, but does not require any TSP lawsuits to be stayed.

Comparison of Retroactive Immunity Provisions

Timing of Certifications

Although alternative proposals to retroactive immunity followed the same general procedure as the FISA Amendments Act with respect to *how* and *by whom* a certification is made, the question of *when* a certification is made may vary substantially. Generally, the certification would appear to be permissible at any stage of litigation before final judgment. Note, however, that the act requires certifications to be made to the court in which the *action is pending*. That clause could possibly be read to disallow certifications in anticipation of any litigation. In contrast, the Senate amendment to H.R. 3773 did not appear to contain such language. The import of this difference may be magnified as a change in Administration is imminent. This may create the possibility that, under the law as passed, a potential plaintiff could forestall filing suit in the hope that a new Administration, opposed to retroactive immunity, would take office. If anticipatory certifications are not permitted because no action is pending, suits filed after the Administration changes could still be dismissed, but only at the discretion of a newly appointed Attorney General.

Similarly, the delay proposed by S.Amdt. 5066 also raised the possibility that a change in Administration could have affected the certification of a lawsuit alleging that participation in the TSP was unlawful. S.Amdt. 5066 would have disallowed certifications until 90 days *after* a report detailing the specifics of the TSP is received by Congress. Depending upon how long it actually took for that report to be completed, certifications might not have been permissible until some time after the current Administration had left office.

Standards of Review

The Senate amendment to H.R. 3773 would have instructed the court to review certifications using an "abuse of discretion standard." In contrast, the enacted FISA Amendments Act requires certifications to be supported by "substantial evidence." Two important characteristics of any standard of review are the level of scrutiny given and the scope of the universe in which such review takes place. An analysis of each standard of review and its potential effect on the pending litigation at issue is discussed below.

Abuse of Discretion. In the judicial context, appellate courts commonly review discretionary rulings of lower courts under an abuse of discretion standard. For example, a federal trial judge's decision to exclude evidence because it is unfairly prejudicial is reversible error only if the trial court made an error of law or acted in

an unprincipled, arbitrary, or irrational manner.[42] In the words of the Supreme Court, it is "deference that is the hallmark of abuse of discretion review."[43]

But, the Senate amendment to H.R. 3773 deals with judicial review of the actions of an executive branch official, namely the Attorney General. Therefore, an examination of the standards for judicial review of administrative action under the Administrative Procedure Act (APA) may be more illustrative than comparisons to review of actions by lower courts. Unless specifically excluded from review by statute, the APA authorizes courts to set aside agency actions that are "arbitrary, capricious, or *an abuse of discretion*."[44] The Supreme Court of the United States had the opportunity to expound upon the meaning of this standard in *Citizens to Preserve Overton Park, Inc. v. Volpe*, a case involving a challenge to the construction of a highway through a public park.[45] The Court held that this standard of review required the reviewing court to

> consider whether the decision was based upon a consideration of the relevant factors and whether there has been a clear error of judgment. Although this inquiry into the facts is to be searching and careful, the ultimate standard of review is a narrow one. The court is not empowered to substitute its judgment for that of the agency.[46]

Therefore, in the case of certifications by the Attorney General, a court reviewing for an abuse of discretion would have likely examined the Attorney General's consideration of the assistance provided by the defendants, the types of representations made by intelligence officials concurrently with requests for assistance, and the facts surrounding any other findings required by the certification.

Note that the Senate amendment to H.R. 3773 did not indicate what record, if any, the court would be able to review in gauging the propriety of the Attorney General's certification. The only documentation the Attorney General would have been required to present is the certification itself, and no other provision would have allowed opposing parties to present contradictory evidence or arguments. Because of these limitations, it is not clear on what basis, if any, a court could have found a certification under H.R. 3773 to be an abuse of discretion.

Substantial Evidence. In contrast, "substantial evidence" is a standard of review frequently used by courts to review formal *findings of fact* by federal

---

[42] *See, e.g., Republic of the Phil. v. Pimentel*, 128 S. Ct. 2180, 2189 (2008); *United States v. York*, 933 F.2d 1343 (7th Cir. 1991); *United States v. Coiro*, 922 F.2d 1008 (2nd Cir. 1991).

[43] *G.E. v. Joiner*, 522 U.S. 136, 143 (1997) (addressing whether appellate court properly evaluated trial court's actions using an abuse of discretion standard).

[44] 5 U.S.C. § 706(2)(A).

[45] *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402 (1971) (overruled on other grounds by *Califano v. Sanders*, 430 U.S. 99, 105 (1977)).

[46] *Id.* at 416.

agencies.[47] It is less stringent than *de novo* review, which would allow a court to look at the evidence anew and come to its own conclusions. Nevertheless, the Supreme Court has described "substantial evidence" as requiring "more than a mere scintilla" of support and comparable to the standard a trial judge must meet to sustain a jury's verdict.[48] In the federal courts, a jury verdict will not be disturbed if "reasonable and fair-minded persons in exercise of impartial judgment" might have come to the same conclusion as the jury.[49] Therefore, under the "substantial evidence" test, if a court reviewing an Attorney General's certification under the FISA Amendments Act found that an objectively reasonable person *could* conclude that the facts in the certification were true, the court would be required to dismiss the suit.

In the administrative context, substantial evidence review and abuse of discretion review occur in factually distinct circumstances. Substantial evidence is required when an agency engages in either formal rulemaking or an adjudicatory hearing. In contrast, abuse of discretion applies in cases of informal rulemaking and decisions. Therefore, it may be difficult to directly compare the two standards in terms of stringency. Although some courts appear to consider substantial evidence a more demanding standard than abuse of discretion, the consistent theme of both standards is that the court is not free to substitute its judgment in place of the agency's.[50] However, any apparent similarity between the level of deference afforded by a reviewing court under either standard should not overshadow important differences in the scope of the record available to the court.

The scope of the record viewed by the court is a critical factor affecting the search for "substantial evidence." In *Universal Camera v. National Labor Relations Board*, the Supreme Court interpreted the Taft-Hartley Act's use of the phrase "substantial evidence *on the record considered as a whole*."[51] A previous version of the act stated only that findings by the National Labor Relations Board be "supported by evidence" and had been read by some courts to mean that if *any* evidence exists to support the agency's findings, then they are valid, regardless of what contradictory evidence also exists. But, in *Universal Camera*, the Supreme Court found that the addition of the phrase "on the record considered as a whole" indicated that Congress intended courts to review agency findings of fact based upon a holistic view of the

---

[47] In *Overton Park*, the Supreme Court remarked that substantial evidence review was not appropriate because the agency had not taken undertaken formal rulemaking or an adjudicatory hearing. *Overton Park*, 401 U.S. at 414.

[48] *Consolidated Edison Co. v. NLRB*, 305 U.S. 197, 229 (1938); *NLRB v. Columbian Enameling & Stamping Co.*, 306 U.S. 292, 300 (1939)

[49] *E.g.*, *Kosmynka v. Polaris Industries, Inc.*, 462 F.3d 74, 79-82 (2nd Cir. 2006) (upholding jury's finding that a manufacturer was negligent for failing to warn that its all-terrain vehicle might upend itself despite uncontested evidence that the manufacturer had received no reports of such incidents).

[50] *See, e.g.*, *Frontier Fishing Corp. v. Evans*, 429 F. Supp. 2d 316, n.7 (citing *Indus. Union Dep't v. API*, 448 U.S. 607, 705 (1980) (Marshall, J., dissenting, asserting that substantial evidence is more stringent, but is ultimately a deferential standard)).

[51] *Universal Camera v. NLRB*, 340 U.S. 474 (1951) (emphasis added).

record, evaluating supporting evidence in light of available contradictory information.[52]

The FISA Amendments Act requires that certifications be supported by "substantial evidence *provided to the court pursuant to this section.*" The act goes on to permit a reviewing court to examine documentation, certifications, briefs and arguments submitted by all parties when determining if substantial evidence supports the certification. One could reasonably conclude that the availability of contradictory evidence would indicate the intent to apply the more stringent *Universal Camera* definition of substantial evidence. On the other hand, the text of the act may not *require* the court to consider extraneous material.[53]

Therefore, as compared with the Senate amendment to H.R. 3773, the FISA Amendments Act provides the possibility of a broader factual record in which to conduct judicial review of a certification by the Attorney General, but may leave much of the discretion to view that record to the court itself. Under the FISA Amendments Act, it seems possible that a court could lawfully dismiss a case upon certification by the Attorney General, if the court finds the substantial evidence standard is satisfied after looking *only* at the information provided by the Attorney General.

---

[52] *Id.* at 490.

[53] *Compare*, 50 U.S.C. § 1885a(b)(2) ("the court *may* examine [supplemental materials]") (emphasis added) *with* 50 U.S.C. § 1185a(c) ("the court *shall* review such certification and the supplemental materials *in camera* and *ex parte*") (emphasis added).