
# Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information

**name redacted**
Legislative Attorney

**name redacted**
Legislative Attorney

January 5, 2006

**Congressional Research Service**
7-....
www.crs.gov
R40888

**CRS Report for Congress**
*Prepared for Members and Committees of Congress*

# Summary

The Revelations in December 2005 that President Bush had authorized the National Security Agency (NSA) to collect signals intelligence from communications involving U.S. persons within the United States, without obtaining a warrant or court order, raised numerous questions regarding the President's authority to order warrantless electronic surveillance. President Bush stated that he believes his order to be fully supported by the Constitution and the laws of the United States, and Attorney General Gonzales clarified that the Administration based its authority both on inherent presidential powers and the joint resolution authorizing the use of "all necessary and appropriate force" to engage militarily those responsible for the terrorist attacks of September 11, 2001 ("AUMF"). Although the resolution does not expressly specify what it authorizes as "necessary and appropriate force," the Administration discerned the intent of Congress to provide the statutory authority necessary to take virtually any action reasonably calculated to prevent a terrorist attack, including by overriding at least some statutory prohibitions that contain exceptions for conduct that is "otherwise authorized by statute." Specifically, the Administration asserts that a part of the Foreign Intelligence Surveillance Act (FISA) that punishes those who conduct "electronic surveillance under color of law except as authorized by statute" does not bar the NSA surveillance at issue because the AUMF is just such a statute. On December 22, 2005, the Department of Justice Office of Legislative Affairs released a letter to certain members of the House and Senate intelligence committees setting forth in somewhat greater detail the Administration's position with regard to the legal authority supporting the NSA activities described by the President.

This report lays out a general framework for analyzing the constitutional and statutory issues raised by the NSA electronic surveillance activity. It then outlines the legal framework regulating electronic surveillance by the government, explores ambiguities in those statutes that could provide exceptions for the NSA intelligence-gathering operation at issue, and addresses the arguments that the President possesses inherent authority to order the operations or that Congress has provided such authority.

This report supersedes CRS memorandum product WD00002, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by (name redacte d) and (name redacted).

# Contents



## Contacts

Recent media revelations that the President authorized the National Security Agency (NSA) to collect signals intelligence[1] from communications involving U.S. persons within the United States, without obtaining a warrant or court order,[2] raise numerous questions regarding the President's authority to order warrantless electronic surveillance. Little information is currently known about the full extent of the NSA domestic surveillance, which was revealed by the New York Times in December, 2005, but allegedly began after the President issued a secret order in 2002. Attorney General Alberto Gonzales laid out some of its parameters, telling reporters that it involves "intercepts of contents of communications where one ... party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."[3] The aim of the program, according to Principal Deputy Director for National Intelligence General Michael Hayden, is not "to collect reams of intelligence, but to detect and warn and prevent [terrorist] attacks."[4]

The President has stated that he believes his order to be fully supported by the Constitution and the laws of the United States,[5] and the Attorney General clarified that the Administration bases its authority both on inherent presidential powers and the joint resolution authorizing the use of "all necessary and appropriate force" to engage militarily those responsible for the terrorist attacks of

---

[1] "Signals intelligence" is defined in the DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, Joint Publication 1-02 (April 12, 2001), as follows:

> 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. . . .

*Id.* at 390 (cross-references omitted). "Communications intelligence" is defined as "Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT." *Id.* at 84. "Electronic intelligence" is defined as "Technical and geolocation intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT.... " *Id.* at 140 (cross-references omitted). "Foreign instrumentation signals intelligence" is defined as:

> Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. . . .

*Id.* at 167 (cross-references omitted).

[2] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 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").

[3] *See* Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) (hereinafter Gonzales Press Conference), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html. The Attorney General emphasized that his discussion addressed the legal underpinnings only for those operational aspects that have already been disclosed by the President, explaining that "the program remains highly classified; there are many operational aspects of the program that have still not been disclosed and we want to protect that because those aspects of the program are very, very important to protect the national security of this country." *Id.*

[4] *Id.*(describing the program as more "aggressive" than traditional electronic surveillance under FISA, but also as "less intrusive").

[5] President Bush's Radio Address of December 17, 2005, *excerpted in 'A Vital Tool,'* USA TODAY, December 19, 2005, at A12.

September 11, 2001 ("AUMF").[6] Although the resolution does not expressly specify what it authorizes as "necessary and appropriate force," the Administration discerns the intent of Congress to provide the statutory authority necessary take virtually any action reasonably calculated to prevent a terrorist attack, including by overriding at least some statutory prohibitions that contain exceptions for conduct that is "otherwise authorized by statute." Specifically, the Administration asserts that a part of the Foreign Intelligence Surveillance Act (FISA)[7] that punishes those who conduct "electronic surveillance under color of law *except as authorized by statute*"[8] does not bar the NSA surveillance at issue because the AUMF is just such a statute.[9] On December 22, 2005, the Department of Justice Office of Legislative Affairs released a letter to certain members of the House and Senate intelligence committees setting forth in somewhat greater detail the Administration's position with regard to the legal authority supporting the NSA activities described by the President.[10]

The Administration's views have been the subject of debate. Critics challenge the notion that federal statutes regarding government eavesdropping may be bypassed by executive order, or that such laws were implicitly superceded by Congress's authorization to use military force. Others, however, have expressed the view that established wiretap procedures are too cumbersome and slow to be effective in the war against terrorism, and that the threat of terrorism justifies extraordinary measures the President deems appropriate, and some agree that Congress authorized the measures when it authorized the use of military force.

This memorandum lays out a general framework for analyzing the constitutional and statutory issues raised by the NSA electronic surveillance activity. It then outlines the legal framework regulating electronic surveillance by the government, explores ambiguities in those statutes that could provide exceptions for the NSA intelligence-gathering operation at issue, and addresses the arguments that the President possesses inherent authority to order the operations or that Congress has provided such authority.

---

[6] Authorization for Use of Military Force ("the AUMF"), P.L. 107-40, 115 Stat. 224 (2001). Attorney General Gonzales explained

> Justice O'Connor ... said, it was clear and unmistakable that the Congress had authorized the detention of an American citizen captured on the battlefield as an enemy combatant for the remainder—the duration of the hostilities. So even though the authorization to use force did not mention the word, 'detention,' she felt that detention of enemy soldiers captured on the battlefield was a fundamental incident of waging war, and therefore, had been authorized by Congress when they used the words, 'authorize the President to use all necessary and appropriate force.'
>
> For the same reason, we believe signals intelligence is even more a fundamental incident of war, and we believe has been authorized by the Congress. And even though signals intelligence is not mentioned in the authorization to use force, we believe that the Court would apply the same reasoning to recognize the authorization by Congress to engage in this kind of electronic surveillance.

Gonzales Press Conference, *supra* note 3.

[7] P.L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978), codified as amended at 50 U.S.C. §§ 1801 *et seq*.

[8] 50 U.S.C. § 1809 (emphasis added).

[9] *See* Gonzales Press Conference, *supra* note 3.

[10] Letter from Assistant Attorney General William E. Moschella to Chairman Roberts and Vice Chairman Rockefeller of the Senate Select Committee on Intelligence and Chairman Hoekstra and Ranking Minority Member Harman of the House Permanent Select Committee on Intelligence (Dec. 22, 2005) (hereinafter "OLA Letter").

# Constitutional Separation of Powers

Foreign intelligence collection is not among Congress's powers enumerated in Article I of the Constitution, nor is it expressly mentioned in Article II as a responsibility of the President. Yet it is difficult to imagine that the Framers intended to reserve foreign intelligence collection to the states or to deny the authority to the federal government altogether. It is more likely that the power to collect intelligence resides somewhere within the domain of foreign affairs and war powers, both of which areas are inhabited to some degree by the President together with the Congress.[11]

The *Steel Seizure Case*[12] is frequently cited as providing a framework for the courts to decide the extent of the President's authority, particularly in matters involving national security. In that Korean War-era case, the Supreme Court declared unconstitutional a presidential order seizing control of steel mills that had ceased production due to a labor dispute, an action justified by President Truman on the basis of wartime exigencies and his role as Commander-in-Chief,[13] despite the fact that Congress had considered but rejected earlier legislation that would have authorized the measure,[14] and that other statutory means were available to address the steel shortage.[15] The Court remarked that

> It is clear that if the President had authority to issue the order he did, it must be found in some provision of the Constitution. And it is not claimed that express constitutional language grants this power to the President. The contention is that presidential power should be implied from the aggregate of his powers under the Constitution. Particular reliance is placed on provisions in Article II which say that 'The executive Power shall be vested in a President ... '; that 'he shall take Care that the Laws be faithfully executed'; and that he 'shall be Commander in Chief of the Army and Navy of the United States.'
>
> The order cannot properly be sustained as an exercise of the President's military power as Commander in Chief of the Armed Forces. The Government attempts to do so by citing a number of cases upholding broad powers in military commanders engaged in day-to-day

[11] The Constitution specifically gives to Congress the power to "provide for the common Defence," U.S. CONST. Art. I, § 8, cl. 1; to "declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water," *id*. § 8, cl. 11; "To raise and support Armies," and "To provide and maintain a Navy," *id.* § 8, cls. 12-13; "To make Rules for the Government and Regulation of the land and naval Forces," *id.* § 8, cl. 14, "To declare War," id. § 8, cl. 1; and to "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof," *id.* § 8, cl. 18. The President is responsible for "tak[ing] Care that the Laws [are] faithfully executed," Art. II, § 3, and serves as the Commander-in-Chief of the Army and Navy, *id*. § 2, cl. 1.

[12] Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952).

[13] *Id.* at 582 (explaining the government's position that the order to seize the steel mills "was made on findings of the President that his action was necessary to avert a national catastrophe which would inevitably result from a stoppage of steel production, and that in meeting this grave emergency the President was acting within the aggregate of his constitutional powers as the Nation's Chief Executive and the Commander in Chief of the Armed Forces of the United States.").

[14] *Id.* at 586 (noting that "[w]hen the Taft-Hartley Act was under consideration in 1947, Congress rejected an amendment which would have authorized such governmental seizures in cases of emergency").

[15] *Id.* at 585. The Court took notice of two statutes that would have allowed for the seizure of personal and real property under certain circumstances, but noted that they had not been relied upon and the relevant conditions had not been met. In particular, the Court dismissed the government's reference to the seizure provisions of § 201 (b) of the Defense Production Act, which the government had apparently not invoked because it was "'much too cumbersome, involved, and time-consuming for the crisis which was at hand.'" *Id*. at 586.

> fighting in a theater of war. Such cases need not concern us here. Even though 'theater of war' be an expanding concept, we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production. This is a job for the Nation's lawmakers, not for its military authorities.[16]

The Court also rejected the argument that past similar assertions of authority by presidents bolstered the executive claims of constitutional power:

> It is said that other Presidents without congressional authority have taken possession of private business enterprises in order to settle labor disputes. But even if this be true, Congress has not thereby lost its exclusive constitutional authority to make laws necessary and proper to carry out the powers vested by the Constitution 'in the Government of the United States, or any Department or Officer thereof.'[17]

The *Steel Seizure Case* is not remembered as much for the majority opinion as it is for the concurring opinion of Justice Robert Jackson, who took a more nuanced view and laid out what is commonly regarded as the seminal explication of separation-of-powers matters between Congress and the President. Justice Jackson set forth the following oft-cited formula:

> 1. When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.... A seizure executed by the President pursuant to an Act of Congress would be supported by the strongest of presumptions and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it.
>
> 2. When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law.
>
> 3. When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.[18]

To ascertain where in this framework the President's claimed authority might fall appears to require a determination of the Congress's will and an assessment of how the Constitution allocates the asserted power between the President and Congress, if at all. If the Constitution forbids the conduct, then the court has a duty to find the conduct invalid, even if the President and Congress have acted in concert. In the absence of a constitutional bar, Congress's support matters, except in the rare case where the President alone is entrusted with the specific power in question.

[16] *Id.* at 587.

[17] *Id.* at 589.

[18] *Id.* at 637-38 (Jackson, J., concurring) (footnotes and citations omitted).

In other words, under this view, the President may sometimes have the effective power to take unilateral action in the absence of any action on the part of Congress to indicate its will, but this should not be taken to mean that the President possesses the inherent authority to exercise full authority in a particular field without Congress's ability to encroach.

William Rehnquist, at the time an Associate Justice of the Supreme Court, took the opportunity in *Dames & Moore v. Regan*[19] to refine Justice Jackson's formula with respect to the cases falling within the second classification, the "zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain."[20]

> In such a case the analysis becomes more complicated, and the validity of the President's action, at least so far as separation-of-powers principles are concerned, hinges on a consideration of all the circumstances which might shed light on the views of the Legislative Branch toward such action, including "congressional inertia, indifference or quiescence."[21]
>
> [I]t is doubtless the case that executive action in any particular instance falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition. This is particularly true as respects cases such as the one before us, involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail.[22]

In *Dames & Moore*, petitioners had challenged President Carter's executive order establishing regulations to further compliance with the terms of an executive agreement he had entered into for the purpose of ending the hostage crisis with Iran. The orders, among other things, directed that legal recourse for breaches of contract with Iran and other causes of action must be pursued before a special tribunal established by the Algiers Accords. President Carter relied largely on the International Economic Emergency Powers Act (IEEPA),[23] which provided explicit support for most of the measures taken, but could not be read to authorize actions affecting the suspension of claims in U.S. courts. The Carter Administration also cited the broad language of the Hostage Act, which states that "the President shall use such means, not amounting to acts of war, as he may think necessary and proper to obtain or effectuate the release" of the hostages.[24] Justice Rehnquist wrote for the majority

> Although we have declined to conclude that the IEEPA or the Hostage Act directly authorizes the President's suspension of claims for the reasons noted, we cannot ignore the general tenor of Congress' legislation in this area in trying to determine whether the President is acting alone or at least with the acceptance of Congress. As we have noted, Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take or every possible situation in which he might act. Such failure of Congress specifically to delegate authority does not, "especially ... in the areas of foreign policy and national security," imply "congressional disapproval" of action taken by the Executive. On the contrary, the enactment of legislation closely related to the question of the President's authority in a particular case which evinces legislative intent to accord the President broad discretion may be considered to "invite" "measures on independent

[19] 453 U.S. 668 (1981) (citing *Youngstown* at 637).

[20] *Id.* at 668-69.

[21] *Id.*

[22] *Id.* at 669.

[23] P.L. 95-223, 91 Stat. 1626, codified as amended at 50 U.S.C. §§ 1701 *et.seq.*

[24] *Id* at 676 (citing the Hostage Act, 22 U. S. C. § 1732).

> presidential responsibility." At least this is so where there is no contrary indication of legislative intent and when, as here, there is a history of congressional acquiescence in conduct of the sort engaged in by the President.[25]

The Court remarked that Congress's implicit approval of the longstanding presidential practice of settling international claims by executive agreement was critical to its holding that the challenged actions were not in conflict with acts of Congress.[26] The Court cited Justice Frankfurter's concurrence in *Youngstown* stating that "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned ... may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II."[27] Finally, the Court stressed that its holding was narrow:

> We do not decide that the President possesses plenary power to settle claims, even as against foreign governmental entities.... But where, as here, the settlement of claims has been determined to be a necessary incident to the resolution of a major foreign policy dispute between our country and another, and where, as here, we can conclude that Congress acquiesced in the President's action, we are not prepared to say that the President lacks the power to settle such claims.[28]

A review of the history of intelligence collection and its regulation by Congress suggests that the two political branches have never quite achieved a meeting of the minds regarding their respective powers. Presidents have long contended that the ability to conduct surveillance for intelligence purposes is a purely executive function, and have tended to make broad assertions of authority while resisting efforts on the part of Congress or the courts to impose restrictions. Congress has asserted itself with respect to domestic surveillance, but has largely left matters involving overseas surveillance to executive self-regulation, subject to congressional oversight and willingness to provide funds.[29]

# Background: Government Surveillance

Investigations for the purpose of gathering foreign intelligence give rise to a tension between the Government's legitimate national security interests and the protection of privacy interests and First Amendment rights.

## The Fourth Amendment

The Fourth Amendment to the 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 Warrants shall issue, but

[25] *Id.* at 678-79 (internal citations omitted).

[26] *Id.* at 680 (citing the International Claims Settlement Act of 1949, 64 Stat. 13, codified as amended at 22 U.S.C. § 1621 *et seq*. (1976 ed. and Supp. IV)).

[27] *Id* at 686 (citing *Youngstown* at 610-611(Frankfurter, J., concurring)).

[28] *Id.* at 688.

[29] For background on the evolution of U.S. intelligence operations, see CRS Report RL32500, *Proposals for Intelligence Reorganization, 1949-2004*, by (name redacted).

> upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

While the right against unreasonable searches and seizures was originally applied only to tangible things, Supreme Court jurisprudence eventually expanded the contours of the Fourth Amendment to cover intangible items such as conversations. As communications technology has advanced, the technology for intrusion into private conversations has kept pace, as have government efforts to exploit such technology for law enforcement and intelligence purposes. At the same time, the Court has expanded its interpretation of the scope of the Fourth Amendment with respect to such techniques, and Congress has legislated both to protect privacy and to enable the government to pursue its legitimate interests in enforcing the law and gathering foreign intelligence information. Yet the precise boundaries of what the Constitution allows, as well as what it requires, are not fully demarcated, and the relevant statutes are not entirely free from ambiguity.

## The Origin of Wiretap Warrants

In *Katz v. United States*,[30] the Court held for the first time that the protections of the Fourth Amendment extend to circumstances involving electronic surveillance of oral communications without physical intrusion.[31] In response, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[32] to provide for search warrants to authorize electronic surveillance for law enforcement purposes, but prohibiting such surveillance in other instances not authorized by law. The *Katz* Court noted that its holding did not extend to cases involving national security, and Congress did not then attempt to regulate national security surveillance. Title III, as originally enacted, contained an exception. It stated that

> Nothing contained in this chapter or in section 605 of the Communications Act ... shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.... [33]

## Intelligence Surveillance

Several years later, the Supreme Court addressed electronic surveillance for domestic intelligence purposes. In *United States v. United States District Court*, 407 U.S. 297 (1972) (the *Keith* case), the United States sought a writ of mandamus to compel a district judge to vacate an order directing the United States to fully disclose electronically monitored conversations. The Sixth

[30] Katz v. United States, 389 U.S. 347, 353 (1967), *overruling* Olmstead v. United States, 277 U.S. 438 (1928).

[31] *Id.* at 359 n.23.

[32] Pub. L. 90-351, 82 Stat. 211, codified as amended at 18 U.S.C. §§ 2510 *et seq*. For more background see CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by (name redacted) and (name redacted).

[33] 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3). The Supreme Court interpreted this provision not as a conferral or recognition of executive authority, but rather, an indication that Congress had "left presidential powers where it found them." United States v. United States District Court, 407 U.S. 297, 303 (1972). The Senate Judiciary Committee noted, however, that the "highly controversial disclaimer has often been cited as evidence of a congressional ratification of the president's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security." S. REP. NO. 95-604(I), at 6-7 (1978).

Circuit refused to grant the writ,[34] and the Supreme Court granted certiorari and affirmed the lower court decision. The Supreme 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."[35] 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.[36]

The Court held that, in the case of intelligence gathering involving domestic security surveillance, prior judicial approval was required to satisfy the Fourth Amendment.[37] 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."[38] The Court expressed no opinion as to "the issues which may be involved with respect to activities of foreign powers or their agents,"[39] but invited Congress to establish statutory

---

[34] 444 F. 2d 651.

[35] United States v. United States District Court, 407 U.S. 297, 313-14 (1972).

[36] 407 U.S. at 299.

[37] *Id.* at 313-14, 317, 319-20. Thus, the Court stated,

> "These Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch.... The Government argues the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security.... "

*Id.* at 317-18. The Government also argued that such surveillances were for intelligence gathering purposes; that the courts "as a practical matter would have neither the knowledge nor the techniques to determine whether there was probable cause to believe that surveillance was necessary to protect national security;" and that disclosure to a magistrate and court personnel of information involved in the domestic security surveillances "would create serious potential dangers to the national security and to the lives of informants and agents" due to the increased risk of leaks. *Id.* at 318-19. The Court found that "these contentions on behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration," but concluded that a case had not been made for a departure from Fourth Amendment standards. *Id.* at 319-20. Justice Powell also 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." ... *Id.* at 313-14.

[38] *Id.* at 308.

[39] *Id.* at 321-22. The *Keith* Court also stated, "Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers within or without this country." *Id.* at 308.

guidelines.[40] Thus, at least insofar as domestic surveillance is concerned, the Court has recognized that Congress has a role in establishing rules in matters that touch on national security.

Court of appeals decisions following *Keith* met more squarely the issue of warrantless electronic surveillance in the context of foreign intelligence gathering. In *United States v. Brown*,[41] while affirming Brown's conviction for a firearm violation, 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.[42] The Third Circuit, in *United States v. Butenko*,[43] in affirming the district court's denial of an espionage defendant's application for disclosure of wiretap records, concluded that warrantless electronic surveillance was lawful, violating neither Section 605 of the Communications Act[44] nor the Fourth Amendment, if its primary purpose was to gather foreign intelligence information.[45]

---

[40] We recognize that domestic surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III [of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 *et seq.*]. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crimes. Given these potential distinctions between Title III criminal surveillances and those involving domestic security, *Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.* Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.... It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court ... ; and that the time and reporting requirements need not be so strict as those in § 2518. The above paragraph does not, of course, attempt to guide the congressional judgment but rather to delineate the present scope of our own opinion. We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which now constitute Title III. *We do hold, however, that prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.*

407 U.S. at 323-24 (emphasis added). Some of the structural elements mentioned here appear to foreshadow the structure Congress chose to establish for electronic surveillance to gather foreign intelligence information in FISA.

[41] 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974).

[42] *Id.* at 426.

[43] 494 F.2d 593 (3rd Cir. 1974), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974).

[44] P.L. 73-416, Title VII, § 705, formerly Title VI, § 605, 48 Stat. 1103, codified as amended at 47 U.S.C. § 605 (providing that except as authorized in Title III, "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person").

[45] 494 F.2d at 602, 604, and 608. However, it would be unlawful if the interception were conducted on a domestic group for law enforcement purposes. *Id*. at 606.

The Ninth Circuit, in *United States v. Buck*,[46] affirmed the conviction of a defendant found guilty of furnishing false information in connection with the acquisition of ammunition and making a false statement with respect to information required to be kept by a licensed firearm dealer. In responding to Buck's contention on appeal that it was reversible error for the district court to fail to articulate the test it applied in ruling, after an in camera inspection, that the contents of one wiretap did not have to be disclosed to the appellant because it was expressly authorized by the Attorney General and lawful for purposes of gathering foreign intelligence, the Ninth Circuit stated that "[f]oreign security wiretaps" were "a recognized exception to the general warrant requirement and disclosure of wiretaps not involving illegal surveillance was within the trial court's discretion." The court found a determination that the surveillance was reasonable was implicit in the lower court's conclusion.[47]

In its plurality decision in *Zweibon v. Mitchell*,[48] a case involving a suit for damages brought by 16 members of the Jewish Defense League against Attorney General John Mitchell and nine FBI special agents and employees for electronic surveillance of their telephone calls without a warrant, the District of Columbia Circuit took a somewhat different view. The surveillance was authorized by the President, acting through the Attorney General, as an exercise of his authority relating to the nation's foreign affairs and was asserted to be essential to protect the nation and its citizens against hostile acts of a foreign power and to obtain foreign intelligence information deemed essential to the security of the United States. The D.C. Circuit, in a plurality decision, held that a warrant was constitutionally required in such a case involving a wiretap of a domestic organization that was not an agent of a foreign power or working in collaboration with a foreign power posing a national security threat.[49] The court further held that the appellants were entitled to the liquidated damages recovery provided in Title III unless appellees on remand establish an affirmative defense of good faith.[50] While its holding was limited to the facts before it, 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." [51]

---

[46] 548 F.2d 871 (9th Cir. 1977), *cert. denied*, 439 U.S. 890 (1977).

[47] *Id.* at 875-76.

[48] 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

[49] 516 F.2d at 650-55.

[50] *Id.* at 659-73.

[51] *Id.* at 613-14. In the context of the its broad dictum, the court did not clarify what "exigent circumstances" might entail. The court explained its understanding of the distinction between "domestic" and "foreign" as follows:

> Throughout this opinion, "internal security" and "domestic security" will refer to threats to the structure or existence of the Government which originate directly from domestic organizations which are neither agents of nor acting in collaboration with foreign powers, and "internal security" or "domestic security" surveillance will refer to surveillance which is predicated on such threats. "Foreign security" will refer to threats to the structure or existence of the Government which emanate either directly or indirectly from a foreign power, and a "foreign security" surveillance will refer to surveillance which is predicated on such threats. A surveillance is a foreign security surveillance regardless of the stimulus that provoked the foreign power; thus the surveillance in this case will be treated as a foreign security surveillance even though the Soviet threats were provoked by actions of a hostile domestic organization. We believe such treatment is required by the limited holding of the Supreme Court in Keith. "National security" will generally be used interchangeably with "foreign security," except where the context makes it clear that it refers to both "foreign security" and "internal security."

*Id*. at 614 n.42 (internal citations omitted).

## Surveillance for Foreign Intelligence Purposes

The Foreign Intelligence Surveillance Act of 1978 (FISA)[52] sought to strike a balance between national security interests and civil liberties. The legislation was a response both to the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (hereinafter the Church Committee) revelations of past abuses of electronic surveillance for national security purposes and to the somewhat uncertain state of the law on the issue. The Church Committee found that every President since Franklin D. Roosevelt had both asserted the authority to authorize warrantless electronic surveillance and had utilized that authority.[53] Concerns over abuses of such authority provided impetus to the passage of the legislation. As the Senate Judiciary Committee noted in its statement of the need for legislation:

> The need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.... While the number of illegal or improper national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillances were regrettably by no means atypical. In 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 ..... past 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.)[54]

The Senate Judiciary Committee also focused on the potentially chilling effect of warrantless electronic surveillance upon the exercise of First Amendment rights:

---

[52] P.L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978), codified as amended at 50 U.S.C. §§ 1801 *et seq*.

[53] *See* S. REP. NO. 95-604(I), at 7, 1978 U.S.C.C.A.N. 3904, 3908. The Senate Judiciary Committee report's "Background" section traces in some detail the history of Executive Branch wiretap practice from the 1930's (after the Supreme Court in *Olmstead* held that the Fourth Amendment did not apply to "intangible" conversations and therefore no warrant was necessary) to the time of the consideration of FISA. *See id.* at 9-15, 1978 U.S.C.C.A.N. at 3911-16. *Olmstead* was overruled by *Katz*, *see supra* note 30 and accompanying text. The report of the House Permanent Select Committee on Intelligence, in its "Background" section, also provides a detailed recitation on the subject in H. REP. NO. 95-1283 at 15-21.

[54] *Id.* at 7-8, 1978 U.S.C.C.A.N. at 3909.

> 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.[55]

The Senate Judiciary Committee stated that the bill was "designed ... to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it," while permitting the legitimate use of electronic surveillance to obtain foreign intelligence information. Echoing the Church Committee, the Senate Judiciary Committee recognized that electronic surveillance has enabled intelligence agencies to obtain valuable and vital information relevant to their legitimate intelligence missions which would have been difficult to acquire by other means.[56]

# Electronic Surveillance: The Current Statutory Framework

The interception of wire, oral, or electronic communications[57] is regulated by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended.[58] Government surveillance for criminal law enforcement is permitted under certain circumstances and in accordance with the procedures set forth in Title III. Government surveillance for the gathering of foreign intelligence information is covered by FISA. These statutes are relevant to the analysis of the legality of the reported NSA surveillance to the extent that their provisions are meant to cover such surveillance, prohibit it, or explicitly exempt it from requirements therein. If Congress meant for FISA to occupy the entire field of electronic surveillance of the type that is being conducted pursuant to the President's executive order, then the operation may fall under the third tier of Justice Jackson's formula, in which the President's "power is at its lowest ebb" and a court could sustain it only by "disabling the Congress from acting upon the subject."[59] In other words, if FISA, together with Title III, were found to occupy the field, then for a court to sustain the President's authorization of electronic surveillance to acquire foreign intelligence information outside the FISA framework, FISA would have to be considered an unconstitutional encroachment on inherent presidential authority. If, on the other hand, FISA leaves room for the

[55] *Id.* at 8, 1978 U.S.C.C.A.N. at 3909-10.

[56] *Id.* at 8-9, 1978 U.S.C.C.A.N. at 3910.

[57] For definitions of "wire communications," "oral communications," and "electronic communications," see 18 U.S.C. § 2510(1), (2), and (12). The latter includes, with certain exceptions, the transfer of any signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic or photooptical system affecting interstate or foreign commerce.

[58] Pub. L. 90-351, 82 Stat. 211, codified as amended at 18 U.S.C. §§ 2510 *et seq*.

[59] Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). *See supra* notes 10 *et seq.*, and accompanying text.

NSA surveillance outside its strictures, then the claimed power might fall into the first or second categories, as either condoned by Congress (expressly or implicitly), or simply left untouched.

## Title III

Title III provides the means for the Attorney General and designated assistants to seek a court order authorizing a wiretap or similar electronic surveillance to investigate certain crimes (18 U.S.C. § 2516). Most other interceptions of electronic communications are prohibited unless the activity falls under an explicit exception. Under 18 U.S.C. § 2511, any person who "intentionally intercepts ... any wire, oral, or electronic communication" or "intentionally uses ... any electronic, mechanical, or other device [that transmits a signal over wire or radio frequencies, or is connected with interstate or foreign commerce] to intercept any oral communication," without the consent of at least one party to the conversation, is subject to punishment or liability for civil damages. The statute also prohibits the intentional disclosure of the contents of an intercepted communication. It prohibits attempts to engage in the prohibited conduct as well as solicitation of other persons to carry out such activity.

Certain exceptions in Title III apply to federal employees and other persons "acting under color of law,"[60] including exceptions for foreign intelligence acquisition. Section 2511 excepts officers, employees, and agents of the United States who, in the normal course of their official duty, conduct electronic surveillance pursuant to FISA (18 U.S.C. § 2511(2)(e)). Furthermore, Congress emphasized in § 1511(2)(f) that

> Nothing contained in [chapters 119 (Title III), 121 (stored wire or electronic surveillance or access to transactional records) or 206 (pen registers and trap and trace devices) of title 18, U.S. Code], or section 705 of the Communications Act of 1934,[61] shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter [119] or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.[62]

[60] Title III also contains some exceptions for private parties, including communications service providers with respect to activity incident to the provision of such service (§ 2511(2)(a)), and for activity related to equipment maintenance and repair, prevention of fraud or unauthorized access, and protection from unlawful interference (§ 2511(2)(g)-(h)). Listening to broadcasts and electronic communications that are available to the general public and not encrypted, such as police band radio, is not prohibited (§ 2511(2)(g)).

[61] 47 U.S.C. § 605 ("[N]o person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception.... ").

[62] 18 U.S.C. § 2511(2)(f), added by the Foreign Intelligence Surveillance Act of 1978 (FISA), § 201(b), P.L. 95-511, 92 Stat. 1783. Prior to this amendment, the section read:

> Nothing contained in this chapter, or section 605 [now 705] of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the

(continued...)

Title III does not define "international or foreign communications" or "domestic." It is unclear under the language of this section whether communications that originate outside the United States but are received within U.S. territory, or vice versa, were intended to be treated as foreign, international or domestic. Recourse to the plain meaning of the words provides some illumination. *Webster's New Collegiate Dictionary* (1977), in pertinent part, defines "international" to mean "affecting or involving two or more nations" or "of or relating to one whose activities extend across national boundaries." Therefore, "international communications" might be viewed as referring to communications which extend across national boundaries or which involve two or more nations. "Foreign" is defined therein, in pertinent part, as "situated outside a place or country; *esp* situated outside one's own country." Thus, "foreign communications" might be interpreted as referring to communications taking place wholly outside the United States. "Domestic" is defined, in pertinent part, in *Webster's* to mean "of, relating to, or carried on within one and esp. one's own country." Therefore, "domestic communications" may be defined as communications carried on within the United States.

The phrase "utilizing a means other than electronic surveillance [under FISA]" could be interpreted as modifying only the clause immediately before it or as modifying the previous clause as well. If it is read not to pertain to the clause regarding acquisition of intelligence from foreign or international communications, then Title III and the other named statutes would not affect the interception of foreign and international communications, whether they are acquired through electronic surveillance within the meaning of FISA or through other means. The legislative history does not support such a reading, however, for two reasons. First, the second clause, relating to intelligence activities involving foreign electronic communications systems,[63] S. REP. NO. 99-541, at 18 (1986). "Proposed chapter 121" refers to FISA. was inserted into the law in 1986 between the first clause and the modifying phrase.[64] It is thus clear that the modifier initially applied to the first clause, and nothing in the legislative history suggests that Congress intended to effect such a radical change as exempting any electronic surveillance involving communications covered by FISA from the procedures required therein. Second, this conclusion is bolstered by the last sentence of the subsection, which specifies that the methods authorized in

---

(...continued)

> exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of wire and oral communications may be conducted.

The Electronic Communications Privacy Act, P.L. 99-508, § 101(c)(1)(A), substituted "wire, oral, or electronic communication" for "wire or oral communications." P.L. 99-508, § 101(b)(3), added the references to "chapter 121," which deals with stored wire and electronic communications and access to transactional records. That subsection also substituted "foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means" for "foreign communications by a means."

[63] The statute does not explain whether "involving a foreign electronic communications system" encompasses only communications that are transmitted and received without ever traversing U.S. wires, cables, or broadcasting equipment, or whether a communication carried primarily by a U.S. carrier that is at any point routed through a non-U.S. communication system "involves" the foreign system. Either way, the interception would have to be carried out pursuant to "otherwise applicable Federal law."

According to the Senate Judiciary Committee, the language was meant

> to clarify that nothing in chapter 119 as amended or in proposed chapter 121 affects existing legal authority for U.S. Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

[64] Electronic Communications Privacy Act of 1986 § 101(b)(3), P.L. 99-508, 100 Stat. 1848 (1986).

FISA and the other statutes are to be the exclusive methods by which the federal government is authorized to intercept electronic communications. Whether given communications are covered by the exclusivity language would require an examination of the definitions of covered communications in Title III and in FISA.[65]

As originally enacted, § 2511 contained what appeared to be a much broader exception for national security intercepts. It excluded from the coverage of Title III surveillance carried out pursuant to the "constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack ... , [and] to obtain foreign intelligence information deemed essential to the security of the United States.... [66] Congress repealed this language when it enacted FISA, and inserted § 2511(2)(f), *supra*, to make the requirements of Title III or FISA the exclusive means to authorize electronic surveillance within the United States, and to "put[] to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in chapters 119 and 120 [of title 18, U.S. Code]."[67] Subsection (2)(f) was intended to clarify that the prohibition does not cover NSA operations (as they were then being conducted) and other surveillance overseas, including that which targets U.S. persons.[68]

## FISA

The Foreign Intelligence Surveillance Act (FISA) provides a framework for the use of "electronic surveillance," as defined in the Act,[69] and other investigative methods[70] to acquire foreign

[65] *See infra* section defining "electronic surveillance."

[66] 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3). The Supreme Court interpreted this provision not as a conferral or recognition of executive authority, but rather, as an indication that Congress had "left presidential powers where it found them." United States v. United States District Court, 407 U.S. 297, 303 (1972). The Senate Judiciary Committee noted, however, that the "highly controversial disclaimer has often been cited as evidence of a congressional ratification of the president's inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security." S. REP. NO. 95-604(I), at 6-7 (1978).

[67] S. REP. NO. 95-604(I), at 64 (1978). Further, the Committee stated, "[a]s to methods of acquisition *which come within the definition of 'electronic surveillance'* in this bill, the Congress has declared that this statute, not any claimed presidential power, controls." *Id.* (emphasis added). The reference to chapter 120 of Title 18, U.S.C., in the report language quoted in the text above is to the foreign intelligence provisions in S. 1566, which became FISA. The Senate version of the measure would have included the foreign intelligence surveillance provisions as a new chapter 120 of Title 18, U.S. Code.

[68] The Senate Judiciary Committee explained that the provision was designed "to make clear the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States." S. REP. NO. 95-604(I), at 64 (1978). The Senate Select Committee on Intelligence echoed this understanding. S. REP. NO. 95-701, at 71 (1978). While legislation then pending that would have regulated these types of operations was not enacted (S. 2525, 95th Cong.), Congress established oversight over such intelligence activities through a review of relevant executive branch procedures and regulations by the House and Senate Intelligence Committees. *See* S. REP. NO. 99-541, at 18 (1986) ("As in the past, the Senate expects that any relevant changes in these procedures and regulations will be provided to the Senate and House Intelligence Committees prior to their taking effect."). The President is also required to report "illegal intelligence activity" to the intelligence committees, 50 U.S.C. § 413(b). "Illegal intelligence activity" is undefined, but legislative history suggests it includes activities that violate the Constitution, statutes, or Executive orders. *See* S. REP. NO. 102-85, at 31 (1991) (explaining that the definition of "illegal intelligence activity" was not changed from the previous version of § 413).

[69] See discussion of the scope of "electronic surveillance" under FISA in the next section of this memorandum, *infra.*

[70] FISA also authorizes the use for foreign intelligence purposes of physical searches, 50 U.S.C. § 1821 *et seq.*; pen registers and trap and trace devices, 50 U.S.C. § 1842 *et seq.*; and orders for production of business records or any tangible thing "for an investigation to obtain foreign intelligence information not concerning a United States person or (continued...)

intelligence information.[71] In pertinent part, FISA provides a means by which the government can obtain approval to conduct electronic surveillance of a foreign power or its agents without first meeting the more stringent standard in Title III that applies to criminal investigations. While Title III requires a showing of probable cause that a proposed target has committed, is committing, or is about to commit a crime, FISA requires a showing of probable cause to believe that the target is a foreign power or an agent of a foreign power.

In the aftermath of the September 11, 2001, terrorist attacks on the United States, Congress amended FISA so that it no longer requires a certification that the (primary) purpose of a search or surveillance is to gather foreign intelligence information.[72] As amended by the USA PATRIOT Act,[73] FISA requires that a "significant purpose" of the investigation be the collection of foreign intelligence information, which has been interpreted to expand the types of investigations that may be permitted to include those in which the primary purpose may be to investigate criminal activity, as long as there is at least a measurable purpose related to foreign intelligence gathering.[74] Congress later enacted a measure that removed, for a time,[75] the requirement for the

(...continued)

to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

[71] "Foreign intelligence information" is defined in FISA, 50 U.S.C. § 1801(e), to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[72] 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*. "Foreign intelligence information" is defined in 50 U.S.C. § 1801(e) to mean:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[73] P.L. 107-56 § 218.

[74] *See In re* Sealed Case, 310 F.3d 717, 735 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002) ("The addition of the word 'significant' to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.").

[75] This amendment, added by section 6001 of the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, 118 (continued...)

government to show that the intended target, if a non-U.S. person, is associated with a foreign power.[76]

## Electronic Surveillance Under FISA

Whether FISA applies to the electronic surveillances at issue turns in large part on the definition of "electronic surveillance" under FISA. To constitute "electronic surveillance" under FISA, the surveillance must fall within one of four categories set forth in 50 U.S.C. § 1801(f), FISA. These include:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person[77] who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio

(...continued)

Stat. 3742 (2004), is subject to the sunset provision of the USA PATRIOT Act. *See* CRS Report RL32186, *USA PATRIOT Act Sunset: Provisions That Were to Expire on December 31, 2005*, by (name redacted).

[76] See CRS Report RS22011, *Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act (FISA)*, by (name redacted) and (name redacted).

[77] "United States person" is defined in 50 U.S.C. § 1801(i) to mean:

> (i) "United States person" means 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.

Under the definition of "foreign power" in 50 U.S.C. § 1801(a), the foreign powers defined in subsections 1801(a)(1), (2), or (3) are either foreign governments or components thereof, factions of a foreign nation or foreign nations which are not substantially composed of U.S. persons, or entities openly acknowledged by a foreign government or governments to be directed and controlled by that government or those governments. These three subsections of the "foreign power" definition do not include international terrorist organizations. *See infra* note 87 for the full definition of "foreign power" under 50 U.S.C. § 1801(a).

> communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[78]

The legislative history of the Act suggests that some electronic surveillance by the National Security Agency involving communications taking place entirely overseas, even involving U.S. persons, was not intended to be covered.[79] At the same time, FISA was clearly meant to cover some communications even if one party to the communication is overseas. The interception of wire or radio communications sent by or intended to be received by a targeted United States person[80] in the United States is covered under 50 U.S.C. § 1801(f)(1). The interception of

---

[78] With respect to the ability of FISA to keep pace with the rapidly changing level of communications technology, it is possible that 50 U.S.C. § 1801(f)(3) and (4) may provide some or all of the needed statutory flexibility. *See, e.g.*, S. REP. NO. 95-604(I) at 34-35, 1978 U.S.C.C.A.N. at 3936, discussing the congressional intent that subsection 1801(f)(4) was intended to be "broadly inclusive, because the effect of including a particular means of surveillance is not to prohibit it but to subject it to judicial oversight." Thus, it was intended to include "the installation of beepers and 'transponders,' if a warrant would be required in the ordinary criminal context.... It could also include miniaturized television cameras and other sophisticated devices not aimed merely at communications." *Id. See* United States v. Andonian, 735 F. Supp. 1469, 1473 (C.D. Cal. 1990), *aff'd and remanded on other grounds*, 29 F.3d 634 (9th Cir. 1994), *cert. denied*, 513 U.S. 1128 (1995).

[79] For example, in discussing the definition of "electronic surveillance," in H.R. 7308, the House Permanent Select Committee on Intelligence stated,

> Therefore, this bill does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally. The committee does not believe that this bill is the appropriate vehicle for addressing this area. The standards and procedures for overseas surveillance may have to be different than those provided in this bill for electronic surveillance within the United States or targeted against U.S. persons who are in the United States.
>
> The fact that this bill does not bring the overseas surveillance and activities of the U.S. intelligence community within its purview, however, should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans. The committee merely recognizes at this point that such overseas surveillance activities are not covered by this bill. In any case, the requirements of the fourth amendment would, of course, continue to apply to this type of communications intelligence activity.

H.REPT. 95-1283(I), at 50-51 (June 5, 1978). The House passed H.R. 7308, amended (Roll No. 737), 124 *Cong. Rec.* 28427 (Sept. 7, 1978). Then the House passed S. 1566, having stricken all but the enacting clause of S. 1566 and having inserted in lieu thereof the text of S. 7308. H.R. 7308 was laid on the table, 124 *Cong. Rec.* 28427-28432 (Sept. 7, 1978).

[80] The House Permanent Select Committee on Intelligence described the import of "intentionally targeting" in the context of subsection (1) of the definition of "electronic surveillance" as follows:

> Paragraph (1) protects U.S. persons who are located in the United States from being targeted in their domestic or *international* communications without a court order no matter where the surveillance is being carried out. The paragraph covers the acquisition of the contents of a wire or radio communication of a U.S. person by intentionally targeting that particular, known U.S. person, provided that the person is located within the United States. Thus, for example, any watchlisting activities of the National Security Agency conducted in the future, directed against the international communications of particular U.S. persons who are in the United States, would require a court order under this provision.
>
> Only acquisition of the contents of those wire or radio communications made with a reasonable expectation of privacy where a warrant would be required for law enforcement purposes is covered by paragraph (1). It is the committee's intent that acquisition of the contents of a wire communication, without the consent of any party thereto, would clearly be included.
>
> The term "intentionally targeting" a particular, known U.S. person who is in the United States includes the deliberate use of a surveillance device to monitor a specific channel of communication which would not be surveilled but for the purpose of acquiring information about a party who is a particular, named U.S. person located within the United States. It also includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous

(continued...)

international wire[81] communications to or from *any* person (whether or not a U.S. person) within the United States without the consent of at least one party is covered under § 1801(f)(2), where the communications are acquired within the United States. The interception of a radio communication is covered under § 1801(f)(3) if all parties to it are located within the United States, unless there is no reasonable expectation of privacy and a warrant would not be required under Title III, even if the interception is acquired by using a device located outside of the United States. The interception of wire, oral, or electronic communications that is not included within the definition of "electronic surveillance" for the purposes of FISA may nevertheless be prohibited by or subject to a warrant requirement pursuant to 18 U.S.C. § 2511 (Title III).

In discussing the repeal in the conforming amendments to FISA of the "national security disclaimer" in former 18 U.S.C. § 2511(3), and the addition of 18 U.S.C. § 2511(f) in the conforming amendments in S. 1566, the Senate Judiciary Committee observed:

> Specifically, this provision is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency[82] and electronic surveillance conducted outside the United States. As to methods of

(...continued)

> parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are selected either by name or by other information which would identify the particular person and would select out his communications.
>
> This paragraph does not apply to the acquisition of the contents of international or foreign communications, where the contents are not acquired by intentionally targeting a particular known U.S. person who is in the United States. . . .

H. REP. NO. 95-1283(I), at 50-51 (June 8, 1978) (emphasis in original).

[81] "Wire communication" means "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(l).

[82] The legislative history of FISA reflects serious concerns about the past NSA abuses reflected in the Church Committee reports. *See, e.g.*, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, UNITED STATES SENATE, S. REP. NO. 94-755, 94th Cong., 2d Sess., at 733-86 (1976), *cited in* S. REP. NO. 95-604(I) at 34 n. 39, 1978 U.S.C.C.A.N. at 3936. Some actions had been taken to address some of these concerns by the President and the Attorney General near the time that FISA was being considered. The decision not to cover NSA activities "as they were then being conducted" in FISA may, in part, have been an acknowledgment of constraints that had been imposed upon some of these practices in E.O. 11905 (Feb. 18, 1976), *cited in* S. REP. NO. 95-604(I) at 34 n. 40, 1978 U.S.C.C.A.N. at 3936; and in the "substantial safeguards [then] currently embodied in classified Attorney General procedures, " H. REP. NO. 95-1283 at 21. In addition, S. 2525 (95th Cong.) was then pending, which, had it passed, would have addressed those areas excluded from FISA in separate legislation. The House Permanent Select Committee also noted the value of congressional oversight in adding an additional safeguard. Nevertheless, the Committee deemed these protections insufficient without the statutory structure in FISA:

> In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties. This committee is well aware of the substantial safeguards respecting foreign intelligence electronic surveillance currently embodied in classified Attorney General procedures, but this committee is also aware that over the past thirty years there have been significant changes in internal executive branch procedures, ant there is ample precedent for later administrations or even the same administration loosening previous standards. Even the creation of intelligence oversight committee should not be considered a sufficient safeguard, for in overseeing classified procedures the committees respect their classification, and the result is that the standards for and limitations on foreign intelligence surveillances may be hidden from public view. In such a situation, the rest of the Congress and the American people need to be assured that the oversight is

(continued...)

> acquisition which come within the definition of 'electronic surveillance' in this bill, the Congress has declared that this statute, not any claimed presidential power, controls.[83]

At the same time, the Committee signaled its intent to reserve its option to regulate U.S. electronic surveillance operations that did not fall within the ambit of FISA:

> The activities of the National Security Agency pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the attorney general during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely during the interim period when these activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed.[84]

## FISA Exceptions to Requirement for Court Order

Three current provisions of FISA provide for some measure of electronic surveillance without a court order to gather foreign intelligence information in specified circumstances, 50 U.S.C. §§ 1802 (electronic surveillance of certain foreign powers without a court order upon Attorney General certification);[85] 1805(f) (emergency authorization of electronic surveillance for up to 72

---

(...continued)

> having its intended consequences–the safeguarding of civil liberties consistent with the needs of national security. While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronic surveillance for foreign intelligence purposes can be conducted.
>
> Finally, the decision as to the standards governing when and how foreign intelligence electronic surveillance should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns–civil liberties and national security. Such a political decision is one properly made by the political branches of Government together, not adopted by one branch on its own and with no regard for the other. Under our Constitution legislation is the embodiment of just such political decisions.

H. REP. NO. 95-1283, at 21-22.

[83] S. REP. NO. 95-604(I) at 62-65, 1978 U.S.C.C.A.N. at 3964-66. *See also* S. REP. NO. 95-701 at 71-72, 1978 U.S.C.C.A.N. at 4040-41.

[84] *Id.*

[85] 50 U.S.C. § 1802 provides:

> (a) (1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—
>
> (A) the electronic surveillance is solely directed at—
>
> (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or
>
> (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title;

(continued...)

hours, while an order approving such surveillance is sought from a judge of the Foreign Intelligence Surveillance Court (FISC));[86] and 1811 (electronic surveillance without a court order for 15 days following a declaration of war by the Congress).

---

(...continued)

> (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and
>
> (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and
>
> if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.
>
> (2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.
>
> (3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless—
>
> (A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or
>
> (B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title.
>
> (4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to—
>
> (A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and
>
> (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain.
>
> The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid.
>
> (b) Applications for a court order under this subchapter are authorized if the President has, by written authorization, empowered the Attorney General to approve applications to the court having jurisdiction under section 1803 of this title, and a judge to whom an application is made may, notwithstanding any other law, grant an order, in conformity with section 1805 of this title, approving electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information, except that the court shall not have jurisdiction to grant any order approving electronic surveillance directed solely as described in paragraph (1)(A) of subsection (a) of this section unless such surveillance may involve the acquisition of communications of any United States person.

[86] The emergency authorization provision in 50 U.S.C. § 1805(f) states:

> (f) Emergency orders
>
> Notwithstanding any other provision of this subchapter, when the Attorney General reasonably determines that—
>
> (1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and

(continued...)

In particular, 50 U.S.C. § 1802 permits the Attorney General to order electronic surveillance without a court order for up to one year to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at means of communications used exclusively between or among foreign powers or on property or premises under the open and exclusive control of a foreign power (the definition here does not include international terrorist organizations)[87]However, for the purpose of § 1802, only subsections 1801(a)(1) through (3) are included. where "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party;" and minimization procedures are put in place.[88] The Attorney General is also required to report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence 30 days in advance. The 30-day requirement can be waived if the Attorney General determines immediate action is required, in which case he is to notify the committees immediately of the minimization procedures and the reason for the urgency. The FISA court is to receive a copy of the certifications under seal.

---

(...continued)

> (2) the factual basis for issuance of an order under this subchapter to approve such surveillance exists;
>
> he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall 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. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

[87] "Foreign power" for purposes of electronic surveillance under FISA is defined in 50 U.S.C. § 1801(a)(1) through (6) as:

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons; or
>
> (6) an entity that is directed and controlled by a foreign government or governments.

[88] "Minimization procedures" are specific procedures implemented with respect to a particular surveillance in order to minimize the acquisition and retention, and prohibit the dissemination, of information concerning unconsenting U.S. persons required to be protected. *See* 50 U.S.C. § 1801(h).

The emergency authorization provision in 50 U.S.C. § 1805(f) authorizes the Attorney General to issue emergency orders to permit electronic surveillance prior to obtaining a court order if the Attorney General determines that emergency conditions make it impossible to obtain an order with due diligence before the surveillance is begun. The Attorney General or his designee must immediately inform a FISA judge and submit a proper application to that judge as soon as practicable, but not more than 72 hours[89] after the Attorney General authorizes such surveillance. Minimization procedures must be followed. In the absence of a judicial order, the surveillance must terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 72 hours from the time the surveillance was authorized. No information obtained or evidence derived from such surveillance may be used as evidence or otherwise disclosed in any trial, hearing, or other government proceeding, and no information concerning any U.S. person may be disclosed at all without that person's consent except with the Attorney General's approval where the information indicates a threat of disaster or serious bodily harm to any person.

Where Congress has passed a declaration of war, 50 U.S.C. § 1811 authorizes the Attorney General to conduct electronic surveillance without a court order for fifteen calendar days following a declaration of war by Congress. This provision does not appear to apply to the AUMF, as that does not constitute a congressional declaration of war.[90] Indeed, even if the authorization were regarded as a declaration of war, the authority to conduct warrantless electronic surveillance under 50 U.S.C. § 1811 would only extend to a maximum of 15 days following its passage.[91]

# The Administration's Position

The Administration's position, as set forth in the Office of Legislative Affairs letter to the leaders of the House and Senate intelligence Committees, is that the President has the constitutional authority to direct the NSA to conduct the activities he described, and that this inherent authority is supplemented by statutory authority under the AUMF.[92] The Administration interprets the AUMF, based on its reading of the Supreme Court opinion in *Hamdi*,[93] as authorizing the President to conduct anywhere in the world, including within the United States, any activity that can be characterized as a fundamental incident of waging war. It includes communications intelligence among the fundamental incidents of waging war. The following sections analyze the extent to which the President's authority to conduct warrantless electronic surveillance is

[89] Section 314(a)(2)(B) of P.L. 107-108, the Intelligence Authorization Act for FY2002, 115 Stat. 1402 (Dec. 28, 2001), H.Rept. 107-328, replaced 24 hours with 72 hours in each place that it appears in 50 U.S.C. § 1805(f).

[90] For a discussion of declarations of war and authorizations for the use of military force, see CRS Report for Congress CRS Report RL31133, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*, by (name redacted) and (name redacted).

[91] This provision originated in the House version of the bill, which would have allowed the President to authorize electronic surveillance for periods up to a year during time of war declared by Congress. The conference substituted a compromise provision authorizing electronic surveillance without a court order to acquire foreign intelligence information for 15 days following a declaration of war. H.R. CONF. REP. NO. 95-1720, at 34 (1978). The 15-day period was intended to "allow time for consideration of any amendment to [FISA] that may be appropriate during a wartime emergency." *Id.* The conferees also expressed their intent that "all other provisions of this act not pertaining to the court order requirement shall remain in effect during this period." *Id.*

[92] OLA Letter, *supra* note 10, at 2.

[93] Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

inherent, whether the AUMF authorizes the operations,[94] and whether the NSA operations are consistent with FISA and Title III.[95]

## The President's Inherent Authority to Conduct Intelligence Surveillance

The statutory language in FISA and the legislative history of the bill that became FISA, S. 1566 (95th Cong.), reflect the Congress's stated intention to circumscribe any claim of inherent presidential authority to conduct electronic surveillance, as defined by the Act, to collect foreign intelligence information, so that FISA would be the exclusive mechanism for the conduct of such electronic surveillance. Thus, in the conforming amendments section of the legislation, the previous language explicitly recognizing the President's inherent authority was deleted from 18 U.S.C. § 2511(3), and the language of 18 U.S.C. § 2511(f) was added to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, which states, in part, that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of that Act, and the interception of domestic wire, oral, and electronic communications may be conducted."[96] The House amendments to the bill provided that the procedures in the bill and in 18 U.S.C., Chapter 119 (Title III), were to be the exclusive "statutory" means by which electronic surveillance as defined in the bill and the interception of domestic wire and oral communications may be conducted, while the Senate bill did not include the word "statutory." The House Conference Report, in accepting the Senate approach, stated, in part, that

> The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure case: "When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter." Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952).[97]

In this language, the conferees acknowledge that the U.S. Supreme Court, as the final arbiter of constitutional power, might reach a different conclusion. The Court has yet to rule on the matter.[98]

---

[94] *See* OLA Letter, *supra* note 10, at 3 ("Because communications intelligence activities constitute, to use the language of *Hamdi*, a fundamental incident of waging war, the AUMF *clearly and unmistakably authorizes* such activities directed against the communications of our enemy.").

[95] We do not address the Administration's argument that the NSA electronic surveillance at issue is compatible with the Fourth Amendment. For analysis pertinent to that issue, see *supra* section on the Background of Government Surveillance.

[96] For further discussion of the pertinent provisions of Title III, see the discussion at notes 54 *et seq*. and accompanying text.

[97] H. CONF. REP. NO. 95-1720, at 35, 1978 U.S.C.C.A.N. at 4064 (Oct. 5, 1978); *see also* S. REP. NO. 95-604(I) at 62-65, 1978 U.S.C.C.A.N. at 3964-66; S. REP. NO. 95-701 at 71-72, 1978 U.S.C.C.A.N. at 4040-41.

[98] However, some lower court decisions provide significant support for the argument that the exclusivity provision circumscribes the President's use of inherent authority to engage in electronic surveillance to collect foreign intelligence information outside the FISA structure. *See, e.g.*, United States v. Andonian, 735 F. Supp. 1469 (C.D. Cal. 1990), *aff'd and remanded on other grounds*, 29 F.3d 634 (9th Cir. 1994), *cert. denied*, 513 U.S. 1128 (1995). The *Andonian* court found that the exclusivity language in FISA

(continued...)

The passage of FISA and the inclusion of such exclusivity language reflects Congress's view of its authority to cabin the President's use of any inherent constitutional authority with respect to warrantless electronic surveillance to gather foreign intelligence. The Senate Judiciary Committee articulated its view with respect to congressional power to tailor the President's use of an inherent constitutional power:

> The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an "inherent" constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.[99]

---

(...continued)

> reveals that Congress intended to sew up the perceived loopholes through which the President had been able to avoid the warrant requirement. The exclusivity clause makes it impossible for the President to 'opt-out' of the legislative scheme by retreating to his 'inherent' Executive sovereignty over foreign affairs. At the time of the drafting of FISA, such a retreat would have meant completely unfettered use of electronic surveillance in the foreign affairs arena, as the Supreme Court had twice declined to hold such Executive action captive to the warrant requirement [citing *Keith*, 407 U.S. 297, *Katz*, 389 U.S. at 358, n. 23, and S. REP. NO. 95-604[(I)] at 12-14, 1978 U.S.C.C.A.N. at 3913-16].... The exclusivity clause in 18 U.S.C. section 2511(2)(f) assures that the President cannot avoid Congress' limitations by resort to 'inherent' powers as had President Truman at the time of the 'Steel Seizure Case.' Youngstown Sheet and Tube v. Sawyer, 343 U.S. 579 (1952).... The difficulty in the case was due to Congressional silence.... When the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, congressional inertia, indifference or acquiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent presidential responsibility. In this area, any actual test of power is likely to depend on the imperatives and events and contemporary imponderables rather than on abstract theories of law.... To foreclose the arguments which piqued the Court in Youngstown, Congress denied the President his inherent powers outright. Tethering executive reign, Congress deemed that the provisions for gathering intelligence in FISA and Title III were 'exclusive.'

*Id*. at 1474-76. *Cf.*, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982). The court stated that

> FISA is the fifth legislative attempt since the Watergate era to bridle the Executive's 'inherent' power. Congress believes that FISA has provided a 'secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.' ... The Act received broad support in Congress and from the then Attorney General Griffin Bell and President Carter.... When, therefore, the President has, as his primary purpose, the accumulation of foreign intelligence information, his exercise of Article II power to conduct foreign affairs is not constitutionally hamstrung by the need to obtain prior judicial approval before engaging in wiretapping. While the executive power to conduct foreign affairs exempts the President from the warrant requirement when foreign surveillance is conducted, the President is not entirely free of the constraints of the Fourth Amendment. The search and seizure resulting from the surveillance must still be reasonable. With the enactment of FISA, ... Congress has fashioned a statute for foreign surveillance that fully comports with the Fourth Amendment.

*Id*. at 1311-12. *See* United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000). The court noted that

> All of the circuit cases finding a foreign intelligence exception [to the warrant requirement] arose before the enactment of FISA (which sets forth procedures for foreign intelligence collection, *see* 50 U.S.C. § 1801 *et seq*.) and are probably now governed by that legislation. FISA only governs foreign intelligence searches conducted within the United States. See 50 U.S.C. §§ 1801(f)(1-4), 1803(a), 1821(5), 1822(c).

*Id*. at 272 n. 8.

[99] S. REP. NO. 95-604(I), at 16, 1978 U.S.C.C.A.N. at 3917. *See also* Attorney General Bell's testimony with respect to (continued...)

On the other hand, the Administration asserts constitutional authority under Article II of the Constitution, including his Commander-in-Chief authority, to order warrantless foreign intelligence surveillance within the United States:

> This constitutional authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits, to have addressed the issue have concluded. *See, e.g., In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. of Review 2002) ("[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.... We take for granted that the President does have that authority.... ").[100]

The U.S. Foreign Intelligence Surveillance Court of Review (Court of Review) was created by FISA, 50 U.S.C. § 1803, and has appellate review over denials of FISA applications by the Foreign Intelligence Surveillance Court which was also established under that section. Denials of such applications by the Court of Review may be appealed to the U.S. Supreme Court. The Court of Review has decided only one published case, which is cited by the Administration above. The case was not appealed to the U.S. Supreme Court. As the Court of Review is a court of appeals and is the highest court with express authority over FISA to address the issue, its reference to inherent constitutional authority for the President to conduct warrantless foreign intelligence surveillance might be interpreted to carry considerable weight.

The Court of Review, in its opinion, make two references which appear pertinent to the Administration's position. The first statement, which is cited by the Administration, was made by the Court of Review, in *In re Sealed Case*,[101] in its discussion of the constitutionality of FISA and its exploration of the underlying rationale of the "primary purpose" test as articulated in *United States v. Truong Dinh Hung*,[102] (which dealt with a pre-FISA surveillance). The Court of Review, in this portion of its constitutional analysis, was considering whether the primary purpose of a FISA electronic surveillance must be to gather foreign intelligence information in order for it to pass constitutional muster. *Truong* saw such a standard as a constitutional minimum. In assessing and rejecting the *Truong* approach, the Court of Review stated:

> It will be recalled that the case that set forth the primary purpose test *as constitutionally required* was *Truong*. The Fourth Circuit thought that *Keith*'s balancing standard implied the adoption of the primary purpose test. We reiterate that *Truong* dealt with a pre-FISA

(...continued)

the Administration's position, *id.* at 4, 1978 U.S.C.C.A.N. at 3905-06; S. REP. NO. 95-701, at 6-7, 1978 U.S.C.C.A.N. at 3975. The need to comply with FISA for the collection of foreign intelligence information through electronic surveillance is reiterated in E.O. 12333 ("United States Intelligence Activities" (December 4, 1981), as amended), Section 2.5, dealing with Attorney General approval required for certain collection techniques:

> 2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

[100] OLA Letter, *supra* note 10, at 2.

[101] 310 F.3d 717 (U.S. Foreign Intell. Surveillance Ct. Rev. 2002).

[102] 629 F.2d 908 (4th Cir. 1980).

> surveillance based on the President's constitutional responsibility to conduct the foreign affairs of the United States. 629 F.2d at 914. Although *Truong* suggested the line it drew was a constitutional minimum that would apply to a FISA surveillance, *see id*. at 914 n. 4, it had no occasion to consider the application of the statute carefully. The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. It was incumbent upon the court, therefore, to determine the boundaries of that constitutional authority in the case before it. *We take for granted that the President does have that authority, and, assuming that is so, FISA could not encroach on the President's constitutional power.* The question before us is the reverse, does FISA amplify the President's power by providing a mechanism that at least approaches a classic warrant and which therefore supports the government's contention that FISA searches are constitutionally reasonable.[103]

While the Court of Review does not cite to the cases to which it is referring, its allusion to the holdings of "all the other courts to have considered the issue," appears to have been to cases which pre-date FISA's passage or which address pre-FISA surveillances.[104] Such cases dealt with a presidential assertion of inherent authority in the absence of congressional action to circumscribe that authority. Where the Congress has exercised its constitutional authority in the areas of foreign affairs and thereby has withdrawn electronic surveillance, as defined by FISA, from the "zone of twilight," between Executive and Legislative constitutional authorities, it might be argued that the President's asserted inherent authority to engage in warrantless electronic surveillance was thereby limited. In the wake of FISA's passage, the Court of Review's reliance on these pre-FISA cases or cases dealing with pre-FISA surveillances as a basis for its assumption

[103] 310 F.3d at 742 (emphasis added).

[104] *Id.* at 742, n. 26; *cf.*, United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) ("Prior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 912-14 (4th Cir.1980), *cert. denied*,454 U.S. 1144 (1982); United States v. Buck, 548 F.2d 871, 875 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir.) (en banc), *cert. denied*,419 U.S. 88 (1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). *But see* Zweibon v. Mitchell, 516 F.2d 594, 633-51 (D.C. Cir. 1975) (dictum), *cert. denied*, 425 U.S. 944 (1976). The Supreme Court specifically declined to address this issue in *United States v. United States District Court*, 407 U.S. 297, 308, 321-22 (1972) (hereinafter referred to as "*Keith*"), but it had made clear that the requirements of the Fourth Amendment may change when differing governmental interests are at stake, *see* Camara v. Municipal Court, 387 U.S. 523 (1967), and it observed in *Keith* that the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations. 407 U.S. at 321-24, 92 S.Ct. at 2138-40."); *Truong Dinh Hung*, 629 F.2d at 914 ("Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs. *See* First National Bank v. Banco Nacional de Cuba, 406 U.S. 759, 765-68, 92 S.Ct. 1808, 1812-1814, 32 L.Ed.2d 466 (1972); Oetjen v. Central Leather Co., 246 U.S. 297, 302, 38 S.Ct. 309, 310, 62 L.Ed. 726 (1918). The President and his deputies are charged by the constitution with the conduct of the foreign policy of the United States in times of war and peace. See United States v. Curtiss-Wright Corp., 299 U.S. 304, 57 S.Ct. 216, 81 L.Ed. 255 (1936). Just as the separation of powers in *Keith* forced the executive to recognize a judicial role when the President conducts domestic security surveillance, 407 U.S. at 316-18, 92 S.Ct. at 2136-2137, so the separation of powers requires us to acknowledge the principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance. In sum, because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance. Accord, United States v. Butenko, 494 F.2d 593 (3 Cir.), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881, 95 S.Ct. 147, 42 L.Ed.2d 121 (1974); United States v. Brown, 484 F.2d 418 (5 Cir. 1973), cert. denied, 415 U.S. 960, 94 S.Ct. 1490, 39 L.Ed.2d 575 (1974); United States v. Clay, 430 F.2d 165 (5 Cir. 1970), *rev'd on other grounds*, 403 U.S. 698, 91 S.Ct. 2068, 29 L.Ed.2d 810 (1971). *Contra*, Zweibon v. Mitchell, 516 F.2d 594 (D.C.Cir.1975) (dictum in plurality opinion in case involving surveillance of domestic organization having an effect on foreign relations but acting neither as the agent of nor in collaboration with a foreign power).").

of the continued vitality of the President's inherent constitutional authority to authorize warrantless electronic surveillance for the purpose of gathering foreign intelligence information might be viewed as somewhat undercutting the persuasive force of the Court of Review's statement.

The second reference to the "President's inherent constitutional authority" in *In re Sealed Case* is in the conclusion to the opinion. Here the Court of Review makes an oblique reference to the President's inherent authority:

> Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from *Keith*, that FISA as amended is constitutional because the surveillances it authorizes are reasonable.[105]

The latter statement was made in support of the Court of Review's conclusion that the procedures for electronic surveillance to gather foreign intelligence information under FISA, as amended by the USA PATRIOT Act, P.L. 107-56, were constitutionally sufficient under Fourth Amendment standards, whether the court orders under FISA were viewed as warrants for Fourth Amendment purposes or not. While not an explicit recognition of presidential inherent constitutional authority, it might be argued that, when viewed in light of the earlier statement, some level of recognition of that authority might also be inferred from this reference.

Both statements were made in a case in which the Court of Review upheld the constitutionality of FISA, an act which, in express legislative language in its conforming amendments to Title III and in its legislative history, was clearly intended to cabin any inherent presidential authority over electronic surveillance within its sweep, and to provide an exclusive structure for the conduct of such electronic surveillance. It might be argued that the adoption of one of two possible interpretations of the statement would avoid internal inconsistency within the court's decision. One approach would be to interpret these statements by the Court of Review as referring to the President's inherent authority to conduct such surveillances outside the scope of "electronic surveillance" under FISA. In essence, the court's statements would then be seen as a reference to presidential authority over those areas of NSA activities which were intentionally excluded from FISA when it was enacted. Alternatively, it might be argued that the court's statements may refer to continuing exercise of inherent presidential authority within the FISA structure, which the Court of Review found to be constitutional.

In light of the exclusivity language in Title III, 18 U.S.C. § 2511(2)(f) and the legislative history of FISA, it might be argued that electronic surveillance pursuant to FISA is subject to the statutory framework, and does not rely upon an assertion of Presidential inherent authority to support it. Alternatively, it might be contended that, in enacting FISA, the Congress circumscribed the manner in which the President might exercise his inherent constitutional authority with respect to foreign intelligence electronic surveillance, rather than eliminating the President's authority.

As this discussion suggests, while the congressional intent to cabin the President's exercise of any inherent constitutional authority to engage in foreign intelligence electronic surveillance may be

[105] 310 F.3d at 746.

clear from the exclusivity provision in FISA and from the legislative history of the measure, some support may be drawn from the Court of Review's decision in *In re Sealed Case* for the position that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework. Whether such authority may exist only as to those areas which were not addressed by FISA in its definition of "electronic surveillance" or is of broader sweep appears to be a matter with respect to which there are differing views.

## The Authorization to Use Military Force

In the aftermath of the September 11, 2001, attacks, Congress passed a joint resolution authorizing the President to

> use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.[106]

Pursuant to that authority, the President ordered U.S. armed forces to invade Afghanistan for the purpose of rooting out Al Qaeda terrorists and toppling the Taliban government that had provided them safe harbor.

The Administration regards the AUMF as providing the authority to conduct electronic surveillance of the type reported in the press.[107] This conclusion, it argues, is supported by the 2004 Supreme Court decision in *Hamdi v. Rumsfeld*,[108] in which the Supreme Court issued its most thorough interpretation of the AUMF to date.[109] In *Hamdi*, a plurality of the Court affirmed the President's power to detain a U.S. citizen as an "enemy combatant" as part of the necessary force authorized by Congress in the AUMF, despite an earlier statute which provides that no U.S. citizen may be detained except pursuant to an act of Congress.[110] However, the Court appears to have relied on a more limited interpretation of the scope of the AUMF than that which the Administration had asserted in its briefs, and, declaring that a "state of war is not a blank check for the President when it comes to the rights of the Nation's citizens,"[111] the Court clarified that notwithstanding the authorization, such detainees have some due process rights under the U.S. Constitution.[112]

---

[106] Authorization for Use of Military Force ("the AUMF"), P.L. 107-40, 115 Stat. 224 (2001). For a discussion of the scant legislative history accompanying the AUMF, see CRS Report RS22357, *Authorization for Use of Military Force in Response to the 9/11 Attacks (P.L. 107-40): Legislative History*, by (name redacted).

[107] *See* OLA Letter, *supra* note 10.

[108] 542 U.S. 507 (2004).

[109] *See* CRS Report RS21884, *The Supreme Court 2003 Term: Summary and Analysis of Opinions Related to Detainees in the War on Terrorism*, by (name redacted).

[110] 18 U.S.C. § 4001(a). For more background and analysis of that statute, see CRS Report RL31724, *Detention of American Citizens as Enemy Combatants*, by (name redacted); CRS Report RS22130, *Detention of U.S. Citizens*, by (name redacted).

[111] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

[112] *Id.* at 517 (2004).

The Administration's position would seem to rely on at least two assumptions. First, it appears to require that the power to conduct electronic surveillance for intelligence purposes is an essential aspect of the use of military force in the same way that the capture of enemy combatants on the battlefield is a necessary incident to the conduct of military operations. Second, it appears to consider the "battlefield" in the war on terrorism to extend beyond the area of traditional military operations to include U.S. territory. Both assumptions have been the subject of debate.

## The Use of Force

The government finds support in the *Hamdi* decision for its assertion that the AUMF implies authority to conduct electronic surveillance operations as a necessary incident to the use of force. This implied authority, it is urged, provides the statutory authority required to dispense with FISA requirements in the same way the *Hamdi* court found the requirement in the Non-Detention Act (18 U.S.C. § 4001(a)), which prohibits the detention of U.S. citizens except pursuant to an act of Congress, to be satisfied by the AUMF.

There is reason, however, to limit *Hamdi* to actual military operations on the battlefield as that concept is traditionally understood. Justice O'Connor wrote for the plurality that

> we understand Congress' grant of authority for the use of 'necessary and appropriate force' to include the authority to detain for the duration of the relevant conflict, and our understanding is based on longstanding law-of-war principles. If the practical circumstances of a given conflict are entirely unlike those of the conflicts that informed the development of the law of war, that understanding may unravel.[113]

*Hamdi* may be limited to a confirmation that the authorization to employ military force against an enemy army necessarily encompasses the authority to capture battlefield enemies, because such captures are an essential aspect of fighting a battle.[114] International law does not permit the intentional killing of civilians or soldiers who are *hors de combat*, preferring capture as the method of neutralizing enemies on the battlefield.[115] The capture of an enemy combatant is arguably as much a use of force as killing or wounding one. Justice O'Connor wrote for the plurality

> There can be no doubt that individuals who fought against the United States in Afghanistan as part of the Taliban, an organization known to have supported the al Qaeda terrorist network responsible for those attacks, are individuals Congress sought to target in passing the AUMF. We conclude that detention of individuals falling into the limited category we are considering, for the duration of the particular conflict in which they were captured, is so

[113] *Hamdi* at 520.

[114] *Padilla v. Hanft*, another case involving an American citizen detained by the military as an "enemy combatant," could be read as an expansion of the detention authority to encompass persons arrested in the United States, far from any battlefield. 423 F.3d 386 (4th Cir. 2005), *petition for cert. filed*, 74 USLW 3275 (Oct 25, 2005)(NO. 05-533). The Fourth Circuit reversed a lower court's finding that the detention was unlawful, but the appellate finding was based on an understanding that the petitioner had taken up arms against American forces in Afghanistan prior to traveling to the United States with the intent of carrying out acts of terrorism. Whether *Hamdi* would also extend to a person detained as an enemy combatant based wholly on activity carried out within the United States has not been addressed by any court.

[115] *See generally* Department of the Army, FM 27-10, The Law of Land Warfare (1956).

> fundamental and accepted an incident to war as to be an exercise of the "necessary and appropriate force" Congress has authorized the President to use.[116]

While the collection of intelligence is also an important facet of fighting a battle, it is not clear that the collection of intelligence constitutes a use of force. The *Hamdi* plurality cited the Geneva Conventions and multiple authorities on the law of war to reach its conclusion that the capture of combatants is an essential part of warfare.[117] The Administration has not pointed to any authority similar to those cited by the *Hamdi* plurality to support its proposition that signals intelligence is a fundamental aspect of combat. To be sure, there can be little doubt that Congress, in enacting the AUMF, contemplated that the armed forces would deploy their military intelligence assets in Afghanistan or wherever else the conventional aspect of the conflict might spread, but a presumption that the authorization extends to less conventional aspects of the conflict could unravel the fabric of *Hamdi*, especially where measures are taken within the United States. While five Justices were willing to accept the government's argument that the detention of enemy combatants captured on the battlefield[118] is a vital aspect of war-fighting, Justice Thomas alone indicated his agreement with the government's argument that wartime detention is also necessary for intelligence purposes.[119] Justice O'Connor agreed that the law of war supports detention of enemy combatants to prevent their return to the battlefield, but agreed with the petitioner that "indefinite detention for the purpose of interrogation is not authorized."[120]

The boundaries of the authority available under this argument are difficult to discern. May *any* statutory prohibition arguably touching on national security that applies "unless otherwise authorized by statute" be set aside based on the AUMF? Presidential assertions of wartime power have faltered for lack of express congressional approval, especially where civil liberties are implicated.[121] A less expansive interpretation of the AUMF might dictate that "necessary and

---

[116] *Hamdi* at 518. Justice Thomas agreed with this proposition, supplying the fifth vote. *Id.* at 587 ("Although the President very well may have inherent authority to detain those arrayed against our troops, I agree with the plurality that we need not decide that question because Congress has authorized the President to do so.").

[117] *Hamdi* at 518-19.

[118] The *Hamdi* plurality limited its decision to "enemy combatants" as defined to mean "an individual who, it alleges, was 'part of or supporting forces hostile to the United States or coalition partners' in Afghanistan and who 'engaged in an armed conflict against the United States' there." *Hamdi* at 516.

[119] *Id.* at 595 (Thomas, J., dissenting) ("The Government seeks to further [its security] interest by detaining an enemy soldier not only to prevent him from rejoining the ongoing fight. Rather, as the Government explains, detention can serve to gather critical intelligence regarding the intentions and capabilities of our adversaries, a function that the Government avers has become all the more important in the war on terrorism."). Justice Scalia, with Justice Stevens, recognized that the government's security needs include the "need to obtain intelligence through interrogation," but declined to evaluate whether the need could be met within the criminal justice system, noting that such determinations are "beyond ... the Court's competence ... but ... not beyond Congress's." *Id.* at 577-78 (Scalia, J., dissenting).

[120] *Hamdi* at 521. Justices Souter and Ginsberg, while accepting the government's position that the AUMF could be read to authorize actions consonant with the usages of war, rejected the assertion that such usages could be invoked to justify the detention of a captive where the military's actions are incompatible with the law of war. *Id.* at 549-50 (Souter, J., concurring in part and dissenting in part). Justices Scalia and Stevens would have found that a U.S. citizen enjoys the full range of due process rights, the AUMF notwithstanding. *Id.* at 556 (Scalia, J., dissenting).

[121] *Compare* Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579 (1952), *Ex parte* Endo, 323 U.S. 214 (1944) (authority to detain U.S. citizen during war not authorized by implication), *Ex parte* Milligan, 71 U.S. (4 Wall.) 2 (1866) (civilian accused of violating the law of war in non-hostile territory could not be tried by military commission), *and* Little v. Barreme, 6 U.S. (2 Cr.) 170 (1804) (where Congress had authorized as part of a limited war the seizure of vessels bound *to* French ports, the President could not authorize the seizure of vessels coming *from* French ports) *with Ex parte* Quirin, 317 U.S. 1, 26-27 (1942) (President's order establishing military commissions to try enemy combatants for violating the law of war was valid where Congress had recognized military commissions in statute), Hirabayashi v. United States, 320 U.S. 81, 89-90 (1943) (discriminatory wartime curfew implemented by the executive (continued...)

appropriate force" must be read, if possible, to conform to the Constitution and Congress's understanding of what activity constitutes a use of force as opposed to an exercise of authority within the domestic sphere.

## The Domestic Sphere versus Military Operations

Although the lack of a formal declaration of war is not relevant to the existence of an armed conflict and is arguably unnecessary for the President to invoke *some* war powers, it may be argued that a formal declaration makes a difference in determining what law applies within the United States, whether to aliens or citizens.[122] For example, the Alien Enemy Act and the Trading with the Enemy Act (TWEA),[123] both of which regulate the domestic conduct of persons during a war, expressly require a declared war and are not triggered simply by an authorization to use force.[124] The Supreme Court long ago held that the President has no implied authority to promulgate regulations permitting the capture of enemy property located in the United States during hostilities short of a declared war, even where Congress had authorized a "limited" war.[125] More pertinently, FISA contains an exception to its requirements for 15 days after a congressional declaration of war.[126] The inclusion of this exception strongly suggests that Congress intended for FISA to apply even during wartime, unless Congress were to pass new legislation. The fact that Congress amended FISA subsequent to September 11, 2001, in order to maximize its effectiveness against the terrorist threat further bolsters the notion that FISA is intended to remain fully applicable. To conclude otherwise would appear to require an assumption that Congress intended the AUMF to authorize the President to conduct electronic surveillance, even against American citizens not involved in combat, under fewer restrictions than would apply during a declared war, notwithstanding FISA provisions strengthened to take such circumstances into account. Even assuming, for argument's sake, that the NSA operations are necessary to prevent another terrorist attack, a presumption that Congress intended to authorize them does not necessarily follow.

---

(...continued)

branch could be enforced against U.S. citizen where Congress had expressly provided for such enforcement) *and* Korematsu v. United States, 323 U.S. 214 (1944) (same). The Administration cites the *Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), for the proposition that "the President has the responsibility to protect the Nation from further attacks, and the Constitution gives him all necessary authority to fulfill that duty." OLA Letter, *supra* note 10, at 2. The *Prize Cases* have generally been interpreted as supporting an assertion of inherent presidential power to thwart an attack. *See* CONSTITUTION ANNOTATED, S. REP. NO. 108-17, at 328-29. It may, however, be significant that the naval blockade there at issue was instituted prior to Congress's having had the opportunity to take action rather than in the face of a statutory prohibition against such action, and was quickly ratified by Congress. *See id.* at 461-62. Given the Court's tendency to treat the latter question as one calling for judicial avoidance based on the "political question" doctrine, *id.* at 329, it is possible that the question may never reach a fuller exegesis. However, the area has been characterized by concessions between the President and Congress with respect to the scope of authority of each. *See id.*, *id*. at 473-75.

[122] *See Youngstown*, 343 U.S. at 645 (Jackson, J., concurring) (noting that separation-of-powers concerns are "heightened when the Commander-in-Chief's powers are exercised in the domestic sphere").

[123] 50 U.S. App. § 1 *et seq.*

[124] *See generally* CRS Report RL31133, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*, by (name redacted) and (name redacted) (identifying statutes effective only during declared wars or during hostilities).

[125] *See* Brown v. United States, 12 U.S. (8 Cranch) 110 (1814); Little v. Barreme, 6 U.S. (2 Cr.) 170 (1804).

[126] 50 U.S.C. § 1811. The legislative history indicates that the 15-day period was intended to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. CONF. REP. NO. 95-1720, at 34 (1978).

It might be argued that the United States *is* part of the battlefield in the war against terrorism in more than just a metaphorical sense. Proponents of this point of view would argue that the AUMF to authorizes the use of force anywhere in the world,[127] including the territory of the United States, against any persons determined by the President to have "planned, authorized, committed, or aided the terrorist attacks" or "harbored such organizations or persons." Under this view, the United States is under actual and continuing enemy attack, and the President has the authority to conduct electronic surveillance in the same way the armed forces gather intelligence about the military operations of enemy forces, even if no actual combat is taking place. After all, intelligence efforts are aimed at identifying an attack before it occurs. If electronic surveillance is considered to be a use of force, the AUMF would seem to limit it to those who "planned, authorized, committed, aided" the Sept. 11 attacks or who "harbored such ... persons." To the extent that the President's executive order authorizes surveillance of persons who are suspected of merely supporting Al Qaeda or affiliated terrorist organizations, it may be seen as being overly broad.

## Are the NSA Electronic Surveillances Consistent with FISA and Title III?

Having concluded that the AUMF authorizes the NSA activity, the Administration finds that the activity meets FISA requirements as well. Although the Administration appears to accept the premise that the surveillance is "electronic surveillance" within the meaning of FISA, it argues that it is excused from following the required procedures because section 109 of FISA[128] exempts from criminal liability those who conduct electronic surveillance without following the FISA procedures where such surveillance is "authorized by statute."

Subsection (a) of section 109 of FISA provides criminal sanctions[129] for a person who intentionally "engages in electronic surveillance under color of law except as authorized by statute;" or who "discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." Under subsection (b), it is a defense to a prosecution under subsection (a) that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction. Under subsection (d), there is federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.[130]

---

[127] *See* Khalid v. Bush, 355 F.Supp.2d 311, 320 (D. D.C. 2005) (noting that "the AUMF does not place geographic parameters on the President's authority to wage this war against terrorists").

[128] 50 U.S.C. § 1809(a)(1).

[129] Subsection (c) provides, "An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both." In light of the general fines provision in 18 U.S.C. § 3571, the maximum fine would appear to be $250,000 for an individual defendant, and $500,000 for an institutional defendant."

[130] Under 50 U.S.C. § 1810, an aggrieved person, other than a foreign power or an agent of a foreign power, as defined in 50 U.S.C. § 1801(a) or (b)(1)(A), who has been subjected to electronic surveillance or about whom information obtained by electronic surveillance of that person has been disclosed or used in violation of 50 U.S.C. § 1809 may bring an action against any person who committed that violation for actual and punitive damages, plus reasonable attorney's fees and other reasonably incurred investigation and litigation costs. Actual damages may not be less than liquidated damages of $1,000 or $100 per day for each day of the violation, whichever is greater.

The language of this section was drawn by the conferees from the House version of the measure, with modifications taken from the Senate version.[131] The House Conference Report, H. CONF. REP. 95-1720, at 33, 1978 U.S.C.C.A.N. at 4062, adopted the House version of these provisions, with amendments to include the Senate provision regarding disclosure or use of information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute. The House Conference Committee described its actions as follows:

> The Senate bill provided, by conforming amendment to title 18, United States Code, for criminal penalties for any person who, under color of law, willfully engages in electronic surveillance except as provided in this bill; for any person who willfully discloses, or endeavors to disclose to any other person information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through unlawful electronic surveillance; and for any person who willfully uses, or endeavors to use, information obtained through unlawful electronic surveillance.
>
> The House amendments provided for separate criminal penalties in this act, rather than by conforming amendment to title 18, for any person who intentionally engages in electronic surveillance under color of law except as authorized by statute. A defense was provided for a defendant who was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.
>
> The conference substitute adopts the House provision modified to add the Senate criminal penalty for any person who discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute. The conferees agree that the criminal penalties for intelligence agents under this Act should be essentially the same as for law enforcement officers under title 18.[132]

---

[131] The Senate Judiciary Committee, in S. REP. NO. 95-604(I), at 61, 1978 U.S.C.C.A.N. at 3962-3963; *see also*, pertinent portion of the Senate Select Committee on Intelligence's S. REP. NO. 95-701, at 68-69, 1978 U.S.C.C.A.N. at 4037-4038, described the Senate version of this provision, which would have provided conforming amendments to Title 18 of the U.S. Code:

> [Section 4(a)(1) and (2) are] ... designed to establish the same criminal penalties for violations of [FISA, conceived in the Senate bill as a new chapter 120 of Title 18, U.S. Code] as apply to violations of chapter 119 [of Title 18, U.S.C.]. As amended, these sections will make it a criminal offense to engage in electronic surveillance except as otherwise specifically provided in chapters 119 and 120. This amendment also provides, however, that "with respect to techniques used by law enforcement officers" which do not involve the actual interception of wire or oral communications, yet do fall within the literal definition of electronic surveillance in Chapter 120 [FISA]—such as the use of a pen register—the procedures of chapter 120 do not apply. In such cases criminal penalties will not attach simply because the government fails to follow the procedures in chapter 120 (such penalties may, of course, attach if the surveillance is commenced without a search warrant or in violation of a court order.) In all cases involving electronic surveillance for the purpose of obtaining foreign intelligence information, however, the prohibitions of 18 U.S.C. 2511 would apply.
>
> (a)(3), (4), (5), and (6). These amendments make clear that the prohibitions in chapter 119 concerning disclosure and use of information, obtained through the interception of wire or oral communications in sections 2511(1)(c) and (d), also apply to disclosure and use of information obtained through electronic surveillance as defined in chapter 120.
>
> The statute calls for a fine of not more than $10,000 or imprisonment for not more than five years, or both, for each violation.

[132] The House Intelligence Committee discussed the meaning of "intentionally" in the context of Section 109(a)(2) of (continued...)

The Administration appears to rely upon the Authorization to Use Military Force (AUMF), P.L. 107-40, 115 Stat. 224 (2001), in arguing that the NSA electronic surveillances at issue are "authorized by statute," as that phrase is used in 50 U.S.C. § 1809(a). The FISA bill as passed included the House version of Section 109(a)(1) of the measure, while Section 109(a)(2) was drawn from the Senate passed bill. The House Permanent Select Committee's Report, H. Rep. No. 95-1283(I), at 96 (June 8, 1978), sheds some light on the intended meaning of Section 109(a)(1) of H.R. 7308 (95th Cong.) which became 50 U.S.C. § 1809(a)(1):

> Section 109(a)(1) carries forward the criminal provisions of chapter 119 [of Title 18, U.S.C.] and makes it a criminal offense for officers or employees of the United States to intentionally engage in electronic surveillance under color of law except as specifically authorized in chapter 119 of title III [of the Omnibus Crime Control and Safe Streets Act of 1968] and this title. Since certain technical activities—such as the use of a pen register—fall within the definition of electronic surveillance under this title, but not within the definition of wire or oral communications under chapter 119 [of Title 18, U.S.C.], the bill provides an affirmative defense to a law enforcement or investigative officer who engages in such an activity for law enforcement purposes in the course of his official duties, pursuant to a search warrant or court order.

The House Permanent Select Committee on Intelligence also noted that, "[o]ne of the important purposes of the bill is to afford security to intelligence personnel so that if they act in accordance with the statute and the court order, they will be insulated from liability; it is not to afford them immunity when they intentionally violate the law."

Thus, the legislative history appears to reflect an intention that the phrase "authorized by statute" was a reference to chapter 119 of Title 18 of the U.S. Code (Title III) and to FISA itself, rather than having a broader meaning, in which case a clear indication of Congress's intent to amend or repeal it might be necessary before a court would interpret a later statute as superceding it. Nevertheless, without taking into account the legislative history, the phrase might be seen as having a more expansive application. This broader view appears to have been taken by the Administration in its position regarding the authority provided by the AUMF.

Next, the Administration turns to the wiretap prohibition contained in Title III, which contains an exception for surveillance carried out pursuant to FISA. Pointing out that the exception in section 109 is broad in comparison to the exception in 18 U.S.C. § 2511, whose prohibition applies "except as otherwise *specifically provided in this chapter*," the Administration appears to conclude that the broader FISA exception subsumes the narrower exception in Title III, at least with respect to national security wiretaps. It cites two of the specific exceptions in Title III. First, 18 U.S.C. 2511(2)(e) provides a defense to criminal liability to government agents who "conduct electronic surveillance, as defined in section 101 of [FISA], as authorized by that Act." The Administration appears to interpret "as authorized by [FISA]" to include activity exempt from the FISA prohibition by virtue of its being authorized by other statute. Under this interpretation,

---

(...continued)

the House bill, which was replaced by the Senate language. However, as the legislative language was written, the word "intentionally" applied to both Section 109(a)(1) and Section 109(a)(2). The House Report, H. REP. NO. 95-1283, at 97, emphasized that "intentionally" as used in this section was "intended to reflect the most strict standard for criminal culpability. What is proscribed is an intentional violation of an order or one of the specified provisions, not just intentional conduct. The Government would have to provide beyond a reasonable doubt both that the conduct engaged in was in fact a violation, and that it was engaged in with a conscious objective or desire to commit a violation.... "

subsection 2511(2)(e) should be read to exempt electronic surveillance "as authorized by FISA *or any other statute*."

Similar analysis leads the Administration to conclude that the Title III exclusivity provision in 18 U.S.C. § 2511(2)(f) poses no impediment. Section 2511(2)(f), which exempts U.S. foreign intelligence activities not covered by FISA, also provides that the procedures in Title III and FISA "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." The Administration argues that

> By expressly and broadly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," section 109 of FISA permits an exception to the "procedures" of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).[133]

In other words, it appears, the FISA "procedures" described in Title III (in 18 U.S.C. § 2511(2)(f)) can include any other procedures authorized, expressly or implicitly, by any other statute, because these would not be prohibited by FISA section 109. This reading would seem to make the exclusivity provision meaningless, a construction not ordinarily favored by courts. It may be questioned whether Congress actually intended for the exception to the criminal prohibition in FISA to negate the more specific requirements in Title III and its exclusivity provision.

The Administration continues

> Some might suggest that FISA could be read to require that a subsequent statutory authorization must come in the form of an amendment to FISA itself. But under established principles of statutory construction, the AUMF and FISA must be construed in harmony to avoid any potential conflict between FISA and the President's Article II authority as Commander in Chief. Accordingly, any ambiguity as to whether the AUMF is a statute that satisfies the requirements of FISA and allows electronic surveillance in the conflict with al Qaeda without complying with FISA procedures must be resolved in favor of an interpretation that is consistent with the President's long-recognized authority.[134]

It is unclear how FISA and the AUMF are seen to collide. Principles of statutory construction generally provide guidance for interpreting Congress's intent with respect to a statute where the text is ambiguous or a plain reading leads to anomalous results; and where possible, a statute that might be read in such a way as to violate the Constitution is to be construed to avoid the violation. However, such principles are only to be applied where there is a genuine ambiguity or conflict between two statutes,[135] and where there is some possible reading that might avoid a conflict.

---

[133] OLA Letter, *supra* note 10, at 3.

[134] *Id.* at 4 (citing *INS v. Cyr*, 533 U.S. 289, 300 v. (2001) (holding that "if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems") (internal citation omitted); *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (noting that a "'cardinal principle' of statutory interpretation [is] that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided'") (citations omitted)). Both cited cases involved due process implications rather than whether a statute violated the principle of separation of powers by encroaching on presidential powers.

[135] *See, e.g,* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1018 (1984) ("Where two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective" (internal quotation marks omitted)).

While the Court has been known to read into a statute language that does not appear, it would be unusual for the Court to read express statutory language out of a statute, except by declaring at least that portion of the statute to be unconstitutional. It would not ordinarily be presumed that Congress meant the opposite of what it said, merely because its words are constitutionally problematic.

It appears that the Administration's views regarding the statutory authorization supporting the NSA activity also rely on an assumption that FISA, at least to the extent that its provisions apply to activity conducted in the war against terrorism, may be an unconstitutional encroachment into presidential powers. Its argument, partly based on the exigencies of the post-9/11 period, seems to imply such a view of FISA:

> As explained above. the President determined that it was necessary following September 11 to create an early warning detection system. FISA could not have provided the speed and agility required for the early warning detection system. In addition, any legislative change, other than the AUMF, that the President might have sought specifically to create such an early warning system would have been public and would have tipped off our enemies concerning our intelligence limitations and capabilities.

Insofar as the Administration's position is founded upon a concern that FISA was not adequate to the needs of the moment, it might be considered whether 50 U.S.C. §§ 1802 (Attorney General certification that certain conditions are met) and 1805(f) (72-hour emergency order), where applicable, may have provided some of the flexibility that the President considered warranted under the circumstances. To the extent that a lack of speed and agility is a function of internal Department of Justice procedures and practices under FISA, it may be argued that the President and the Attorney General could review those procedures and practices in order to introduce more streamlined procedures to address such needs. Where FISA's current statutory framework proved inadequate to the task, legislative changes might be pursued.

The Administration argues that, "any legislative change, other than the AUMF, that the President might have sought specifically to create such an early warning system would have been public and would have tipped off our enemies concerning our intelligence limitations and capabilities."[136] However, some of these concerns may be minimized or addressed by virtue of the fact that, where appropriate, oversight may be conducted in executive session; and access to classified information, including information relating to sensitive intelligence sources and methods, may be limited by statute, by House and Senate procedures, or both. Nevertheless, to some degree, the federal legislative process is, by its very nature, public. Depending upon how such legislation was structured, an argument may be made that it might give rise to some inferences as to present or future intelligence practices or capabilities. On the other hand, the legislative vehicle chosen and the legislative language used might minimize some of those concerns. In addition, no legal precedent appears to have been presented that would support the President's authority to bypass the statutory route when legislation is required, based an asserted need for secrecy.[137]

---

[136] *See* OLA Letter, *supra* note 10, at 5.

[137] *C.f.* Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 603-04 (Frankfurter, J., concurring):

> The utmost that the Korean conflict may imply is that it may have been desirable to have given the President further authority, a freer hand in these matters. Absence of authority in the President to deal with a crisis does not imply want of power in the Government. Conversely the fact that power exists in the Government does not vest it in the President. The need for new legislation does not

(continued...)

# Conclusion

Whether an NSA activity is permissible under the Fourth Amendment and the statutory scheme outlined above is impossible to determine without an understanding of the specific facts involved and the nature of the President's authorization, which are for the most part classified. If the NSA operations at issue are encompassed in the definition of "electronic surveillance" set forth under FISA, it would seem consistent with Congress's intent that such surveillance must be carried out in accordance with FISA procedures. Although section 109(a) of FISA does not explicitly limit the language "as authorized by statute" to refer only to Title III and to FISA, the legislative history suggests that such a result was intended. The exceptions to the criminal prohibition under Title III, however, are specifically limited to those mentioned within Title III. Even if the AUMF is read to provide the statutory authorization necessary to avoid criminal culpability under FISA, it does not necessarily follow that the AUMF provides a substitute authority under FISA to satisfy the more specific language in Title III. To the extent that any of the electronic surveillance at issue may be outside the sweep of FISA or Title III, Congress does not appear to have legislated specifically on the subject, nor, by the absence of legislation, to have authorized or acquiesced in such surveillance.

Whether such electronic surveillances are contemplated by the term "all necessary and appropriate force" as authorized by the AUMF turns on whether they are, under the *Hamdi* analysis, an essential element of waging war. Even assuming that the President's role as Commander in Chief of the Armed Forces is implicated in the field of electronic surveillance for the collection of foreign intelligence information within the United States, it should not be accepted as a foregone conclusion that Congress has no role to play.[138] By including the emergency authorization for electronic surveillance without a court order for fifteen days following a declaration of war, Congress seems clearly to have contemplated that FISA would continue to operate during war, although such conditions might necessitate amendments. Amendments to FISA in the USA PATRIOT Act and subsequent legislation further demonstrate Congress's willingness to make adjustments. The history of Congress's active involvement in regulating electronic surveillance within the United States leaves little room for arguing that Congress has accepted by acquiescence the NSA operations here at issue.

To the extent that the Administration seems to base its interpretation of the AUMF and FISA on the assumption that a reading contrary to the one they rely upon would be an unconstitutional violation of separation-of-powers principles, it appears to regard the matter as deserving the highest level of deference under *Youngstown's* first category[139] simply by virtue of the assumption

(...continued)

> enact it. Nor does it repeal or amend existing law.

[138] *Id.* at 643-44 (Jackson, J., concurring).

> There are indications that the Constitution did not contemplate that the title Commander in Chief of the Army and Navy will constitute him also Commander in Chief of the country, its industries and its inhabitants. He has no monopoly of 'war powers,' whatever they are. While Congress cannot deprive the President of the command of the army and navy, only Congress can provide him an army or navy to command. It is also empowered to make rules for the 'Government and Regulation of land and naval Forces,' by which it may to some unknown extent impinge upon even command functions.

[139] *See* OLA Letter, *supra* note 10, at 3 (asserting that "the President's 'authority is at its maximum,'" under Justice Jackson's concurrence in *Youngstown* and suggesting that the NSA operations contrast with the seizure invalidated in that case, which resulted from "the absence of a statute 'from which [the asserted authority] [could] be fairly implied'" (continued...)

that it would survive scrutiny under the third category. To conclude that Congress's enactments are unconstitutional and therefore could not reflect Congress's intent seems to beg the question.

Court cases evaluating the legality of warrantless wiretaps for foreign intelligence purposes provide some support for the assertion that the President possesses inherent authority to conduct such surveillance. The Court of Review, the only appellate court to have addressed the issue since the passage of FISA, "took for granted" that the President has inherent authority to conduct foreign intelligence electronic surveillance under his Article II powers, stating that, "assuming that was so, FISA could not encroach on that authority."[140] However, much of the other lower courts' discussions of inherent presidential authority occurred prior to the enactment of FISA, and no court has ruled on the question of Congress's authority to regulate the collection of foreign intelligence information.

From the foregoing analysis, it appears unlikely that a court would hold that Congress has expressly or impliedly authorized the NSA electronic surveillance operations here under discussion, and it would likewise appear that, to the extent that those surveillances fall within the definition of "electronic surveillance" within the meaning of FISA or any activity regulated under Title III, Congress intended to cover the entire field with these statutes. To the extent that the NSA activity is not permitted by some reading of Title III or FISA, it may represent an exercise of presidential power at its lowest ebb, in which case exclusive presidential control is sustainable only by "disabling Congress from acting upon the subject."[141] While courts have generally accepted that the President has the power to conduct domestic electronic surveillance within the United States inside the constraints of the Fourth Amendment, no court has held squarely that the Constitution disables the Congress from endeavoring to set limits on that power. To the contrary, the Supreme Court has stated that Congress does indeed have power to regulate domestic surveillance,[142] and has not ruled on the extent to which Congress can act with respect to electronic surveillance to collect foreign intelligence information. Given such uncertainty, the Administration's legal justification, as presented in the summary analysis from the Office of Legislative Affairs, does not seem to be as well-grounded as the tenor of that letter suggests.

## Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....

(...continued)

(citing *Youngstown* at 585)).

[140] 310 F.3d at 742; *see also id.* at 746.

[141] *Id.* at 638.

[142] United States v. United States District Court, 407 U.S. 297, 323-24 (1972).