U.S. Department of Justice

Office of Legal Counsel

Office of the Deputy Assistant Attorney General

Washington, D.C. 20530

May 17, 2002

Judge Colleen Kollar-Kotelly
U.S. District Court for the District of Court
U.S. Courthouse
3d & Constitution Ave., N.W.
Washington, D.C. 20001

Dear Judge:

It was a pleasure to meet you today. I am writing this letter, at the direction of the Attorney General and in the interests of comity between the executive and legislative branches, to follow up on your questions concerning the scope of the President's authority to conduct warrantless searches. In particular, this letter discusses the President's power to deploy expanded electronic surveillance techniques in response to the terrorist attacks against the United States on September 11, 2001. This letter outlines the legal justifications for such surveillance, which could be conducted without a warrant for national security purposes. Under the current circumstances, in which international terrorist groups continue to pose an immediate threat, we have concluded that such surveillance would be reasonable under the Fourth Amendment because it advances the compelling government interest of protecting the Nation from direct attack.

Part I of this memorandum discusses the relevant factual background. Part II examines the legal framework that governs the collection of electronic communications in the United States, and whether warrantless electronic surveillance is consistent with it. Part III reviews different doctrines that affect the legality of different types of surveillance. Part IV discusses the application of the Fourth Amendment in light of the September 11 attacks.

I.

Four coordinated terrorist attacks took place in rapid succession on the morning of September 11, 2001, aimed at critical Government buildings in the Nation's capital and landmark buildings in its financial center. Terrorists hijacked four airplanes: one then crashed into the Pentagon and two in the World Trade Center towers in New York City; the fourth, which was headed towards Washington, D.C., crashed in

Pennsylvania after passengers attempted to regain control of the aircraft. The attacks caused about five thousand deaths and thousands more injuries. Air traffic and communications within the United States have been disrupted; national stock exchanges were shut for several days; damage from the attack has been estimated to run into the billions of dollars. The President has found that these attacks are part of a violent terrorist campaign against the United States by groups affiliated with Al-Qaeda, an organization headed by Usama bin Laden, that includes the suicide bombing attack on the U.S.S. Cole in 2000, the bombing of our embassies in Kenya and Tanzania in 1998, the attack on a U.S. military housing complex in Saudi Arabia in 1996, and the bombing of the World Trade Center in 1993. The nation has undergone an attack using biological weapons, in which unknown terrorists have sent letters containing anthrax to government and media facilities, and which have resulted in the closure of executive, legislative, and judicial branch buildings.

In response, the Government has engaged in a broad effort at home and abroad to counter terrorism. Pursuant to his authorities as Commander-in-Chief and Chief Executive, the President has ordered the Armed Forces to attack al-Qaeda personnel and assets in Afghanistan, and the Taliban militia that harbors them. Congress has provided its support for the use of force against those linked to the September 11, 2001 attacks, and has recognized the President's constitutional power to use force to prevent and deter future attacks both within and outside the United States. S.J. Res. 23, Pub. L. No. 107-40, 115 Stat. 224 (2001). The military has also been deployed domestically to protect sensitive government buildings and public places from further terrorist attack. The Justice Department and the FBI have launched a sweeping investigation in response to the September 11 attacks. In October, 2001, Congress enacted legislation to expand the Justice Department's powers of surveillance against terrorists. By executive order, the President has created a new office for homeland security within the White House to coordinate the domestic program against terrorism.

Electronic surveillance techniques would be part of this effort. The President would order warrantless surveillance in order to gather intelligence that would be used to prevent and deter future attacks on the United States. Given that the September 11 attacks were launched and carried out from within the United States itself, an effective surveillance program might include individuals and communications within the continental United States. This would be novel in two respects. Without access to any non-public sources, it is our understanding that generally the National Security Agency (NSA) only conducts electronic surveillance of communications outside the United States that do not involve United States persons. Usually, surveillance of communications by United States persons within the United States is conducted by the FBI pursuant to a warrant obtained under the Foreign Intelligence Surveillance Act ("FISA"). Second, interception could include electronic messages carried through the internet, which again could include communications within the United States involving United States persons. Currently, it is our understanding that neither the NSA nor law enforcement conducts broad monitoring of electronic communications in this manner within the United States, without specific authorization under FISA.

II.

This Part discusses the legal authorities that govern the intelligence agencies, and whether warrantless electronic surveillance is consistent with them. Section A concludes that while certain aspects of such electronic surveillance might be inconsistent with earlier executive order, a presidential decision to conduct the surveillance constitutes a legitimate waiver to the order and is not unlawful. Section B concludes that the Foreign Intelligence Surveillance Act ("FISA") does not restrict the constitutional authority of the executive branch to conduct surveillance of the type at issue here.

A.

The NSA was formed in 1952 by President Truman as part of the Defense Department. Under Executive Order 12,333, 46 Fed. Reg. 59941 (1981), the NSA is solely responsible for "signals intelligence activities ["SIGINT"]." Id. § 1.12(b)(1). It provides intelligence information acquired through the interception of communications to the White House, executive branch agencies, the intelligence community, and the armed forces for intelligence, counter-intelligence, and military purposes. Clearly, the basic authority for the establishment of the NSA is constitutional: the collections of SIGINT is an important part of the Commander-in-Chief and Chief Executive powers, which enable the President to defend the national security both at home and abroad. While Congress has enacted statutes authorizing the funding and organization of the NSA, it has never established any detailed statutory charter governing the NSA's activities. *See* Intelligence Authorization Act for FY 1993, Pub. L. No. 102-496, sec. 705 (giving Secretary of Defense responsibility to ensure, through the NSA, the "continued operation of an effective unified organization for the conduct of signals intelligence activities").

The NSA generally has limited its operations to the interception of international communications in which no United States person (a United States citizen, permanent resident alien, a U.S. corporation, or an unincorporated association with a substantial number of members who are U.S. citizens or permanent resident aliens) is a participant. According to publicly-available information, the NSA pulls in a great mass of international telephone, radio, computer, and other electronic communications, and then filters them using powerful computer systems for certain words or phrases. *See, e.g., Halkin v. Helms*, 690 F.2d 977, 983-84 (D.C. Cir. 1982). Congress, however, has not imposed any express statutory restrictions on the NSA's ability to intercept communications that involve United States citizens or that occur domestically. This lack of limitations can be further inferred from the National Security Act of 1947. The Act places a clear prohibition, for example, upon the Central Intelligence Agency's domestic activities. While Section 103 of the National Security Act commands the Director of Central Intelligence to "collect intelligence through human sources and by other appropriate means," it also adds "except that the Agency shall have no police, subpoena, or law enforcement powers or internal security functions." 50 U.S.C. § 403-3(d)(1) (1994 & Supp. V 1999). There is no similar provision that applies to the NSA, which implies that the NSA can conduct SIGINT operations domestically.

Rather than from statute, the limitation on the NSA's domestic SIGINT capabilities derives from executive order. Executive Order 12,333 requires that any "[c]ollection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the FBI." Executive Order 12,333, at § 2.3(b). If "significant foreign intelligence is sought," the Executive Order permits other agencies within the intelligence community to collect information "provided that no foreign intelligence collection by such agencies may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons." *Id.* Section 2.4 further makes clear that the intelligence community cannot use electronic surveillance, among other techniques, "within the United States or directed against United States persons abroad" unless they are according to procedures established by the agency head and approved by the Attorney General. In its own internal regulations, the NSA apparently has interpreted these provision as limiting its SIGINT operations only to international communications that do not involve United States persons.

Thus, the question arises whether a presidential decision to conduct warrantless electronic surveillance, for national security purposes, violates Executive Order 12,333, if such surveillance is not limited only to foreign communications that do not involve U.S. citizens. Thus, for example, all communications between United States persons, whether in the United States or not, and individuals in [redacted] might be intercepted. The President might direct the NSA to intercept communications between suspected terrorists, even if one of the parties is a United States person and the communication takes place between the United States and abroad. The non-content portion of electronic mail communications also might be intercepted, even if one of parties is within the United States, or one or both of the parties are non-citizen U.S. persons (i.e., a permanent resident alien). Such operations would expand the NSA's functions beyond the monitoring only of international communications of non-U.S. persons.

B1
B3

While such surveillance may go well beyond the NSA's current operations, it would not violate the text of the Executive Order. Executive Order 12,333 states that "when significant foreign intelligence is sought," the NSA and other agencies of the intelligence community may collect foreign intelligence within the United States. The only qualification on domestic collection is that it cannot be undertaken to acquire information about the domestic activities of United States persons. If United States persons were engaged in terrorist activities, either by communicating with members of Al Qaeda [redacted] or by communicating with foreign terrorists even within the United States, they are not engaging in purely "domestic" activities. Instead, they are participating in foreign terrorist activities that have a component within the United States. We do not believe that Executive Order 12,333 was intended to prohibit intelligence agencies from tracking international terrorist activities, solely because terrorists conduct those activities within the United States. This would create the odd incentive of providing international terrorists with more freedom to conduct their illegal activities *inside* the United States than outside of it. Rather, the Executive Order was meant to protect the privacy of United States persons where foreign threats were not involved. Further, Section 2.4 of Executive Order 12,333 contemplates that the NSA and other

B1
B3

intelligence agencies can collect intelligence within the United States, so long as the Attorney General approves the procedures.

Even if surveillance were to conflicts with Executive Order 12,333, it could not be said to be illegal. An executive order is only the expression of the President's exercise of his inherent constitutional powers. Thus, an executive order cannot limit a President, just as one President cannot legally bind future Presidents in areas of the executive's Article II authority. Further, there is no constitutional requirement that a President issue a new executive order whenever he wishes to depart from the terms of a previous executive order. In exercising his constitutional or delegated statutory powers, the President often must issue instructions to his subordinates in the executive branch, which takes the form of an executive order. An executive order, in no sense then, represents a command from the President to himself, and therefore an executive order does not commit the President himself to a certain course of action. Rather than "violate" an executive order, the President in authorizing a departure from an executive order has instead modified or waived it. Memorandum for the Attorney General, From: Charles J. Cooper, Assistant Attorney General, *Re: Legal Authority for Recent Covert Arms Transfers to Iran* (Dec. 17, 1986). In doing so, he need not issue a new executive order, rescind the previous order, or even make his waiver or suspension of the order publicly known. Thus, here, the October 4, 2001 Authorization, even if in tension with Executive Order 12,333, only represents a one-time modification or waiver of the executive order, rather than a "violation" that is in some way illegal.

B.

Although it would not violate either the statutory authority for the NSA's operations or Executive Order 12,333, warrantless electronic surveillance within the United States, for national security purposes, would be in tension with FISA. FISA generally requires that the Justice Department obtain a warrant before engaging in electronic surveillance within the United States, albeit according to lower standards than apply to normal law enforcement warrants. Indeed, some elements of an electronic surveillance program – such as intercepting the communications of individuals for which probable cause exists to believe are terrorists – could probably be conducted pursuant to a FISA warrant. Here, however, a national security surveillance program could be inconsistent with the need for secrecy, nor would it be likely that a court could grant a warrant for other elements of a surveillance program, such as the monitoring of all calls to and from a foreign nation, or the general collection of communication addressing information. Nonetheless, as our Office has advised before, and as the Justice Department represented to Congress during passage of the Patriot Act of 2001, which resulted in several amendment to FISA, FISA only provides a safe harbor for electronic surveillance, and cannot restrict the President's ability to engage in warrantless searches that protect the national security. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001). The

ultimate test of the October 4 Authorization, therefore, is not FISA but the Fourth Amendment itself.

FISA requires that in order to conduct electronic surveillance for foreign intelligence purposes, the Attorney General must approve an application for a warrant, which is then presented to a special Article III court. If the target of the surveillance is a foreign power, the application need not detail the communications sought or the methods to be used. If the target is an agent of a foreign power, which the statute defines to include someone who engages in international terrorism, 50 U.S.C. § 1801(b)(2)(C) (1994 & Supp. V 1999), the application must contain detailed information concerning the target's identity, the places to be monitored, the communications sought, and the methods to be used. *Id.* at § 1804(a)(3)-(11). After passage of the FISA amendments as part of the Patriot Act, the National Security Adviser must certify that a "significant" purpose of the surveillance is to obtain foreign intelligence information that cannot be obtained through normal investigative techniques. FISA defines foreign intelligence information to include information that relates to "actual or potential attack or other grave hostile acts of a foreign power" or its agent, or information concerning "sabotage or international terrorism" by a foreign power or its agent, or information that, if a United States person is involved, is necessary for the national security or conduct of foreign affairs. *Id.* at § 1801(e).

FISA provides more secrecy and a lower level of proof for warrants. FISA creates a lesser standard than required by the Fourth Amendment for domestic law enforcement warrants, because the Attorney General need not demonstrate probable cause of a crime. He must only show that there is reason to believe that the target is a foreign power or an agent of a foreign power, and that the places to be monitored will be used by them. *Id.* at § 1804(a)(4)(A)-(B). If the target is a United States person, however, the Court must find that the National Security Adviser's certification is not clearly erroneous.

We do not believe an electronic surveillance program, undertaken in response to the September 11, 2001 attacks, could fully satisfy FISA standards. Such a program could seek to intercept all communications between the United States and certain countries where terrorist groups are known to operate, or communications that involve terrorists as participants. An effective surveillance program might not be able to enforce a distinction between United States persons or aliens, or to require that there be any actual knowledge of the identity of the targets of the search. FISA, however, requires that the warrant application identify the target with some particularity, probably either by name or by pseudonym. *Id.* at § 1804(a)(3); *cf. United States v. Principie*, 531 F.2d 1132 (2d Cir. 1976). To the extent that a presidential order would require probable cause to believe that a participant in a communication is a terrorist, this would more than meet FISA standards that the Justice Department show that the subject of a search is an agent of a foreign power. A standard based on reasonable grounds also would probably meet FISA standards. This, however, would not save a surveillance program's interception of all communications between the United States and another country from statutory difficulties.

Further problems are presented by FISA's requirement that the application describe the "places"

or "facilities" that are to be used by the foreign agent. While this requirement clearly extends beyond specific communication nodes, such as phones, to include facilities, we believe it unlikely that FISA would allow surveillance [redacted] Title III of the 1968 Act, for example, also requires the specification of "facilities" in addition to "places," and defines them as devices that transmit communications between two points. The courts have read "facilities" to allow surveillance of multiple telephone lines, rather than just an individual phone. We have not found an example, however, in which a court has granted a Title III warrant that would cover [redacted] which is the object of the surveillance program contemplated here. Thus, it is unlikely that the FISA court would grant a warrant that could authorize an effective surveillance program undertaken in response to the September 11 attacks.

B1
B3

B1
B3

FISA purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence, just as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, claims to be the exclusive method for authorizing domestic electronic surveillance for law enforcement purposes. FISA establishes criminal and civil sanctions for anyone who engages in electronic surveillance, under color of law, except as authorized by statute, warrant, or court order. 50 U.S.C. § 1809-10. It might be thought, therefore, that a warrantless surveillance program, even if undertaken to protect the national security, would violate FISA's criminal and civil liability provisions.

Such a reading of FISA would be an unconstitutional infringement on the President's Article II authorities. FISA can regulate foreign intelligence surveillance only to the extent permitted by the Constitution's enumeration of congressional authority and the separation of powers. FISA itself is not required by the Constitution, nor does it necessarily establish standards and procedures that exactly match those required by the Fourth Amendment. Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001); *cf.* Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). Instead, like the warrant process in the normal criminal context, FISA represents a statutory procedure that creates a safe harbor for surveillance for foreign intelligence purposes. If the government obtains a FISA warrant, its surveillance will be presumptively reasonable under the Fourth Amendment. Nonetheless, as we explained to Congress during passage of the Patriot Act, the ultimate test of whether the government may engage in foreign surveillance is whether the government's conduct is consistent with the Fourth Amendment, not whether it meets FISA.

This is especially the case where, as here, the executive branch possess the inherent constitutional power to conduct warrantless searches for national security purposes. Well before FISA's enactment, Presidents have consistently asserted – and exercised – their constitutional authority to conduct warrantless

searches necessary to protect the national security.[1] This Office has maintained, across different administrations controlled by different political parties, that the President's constitutional responsibility to defend the nation from foreign attack implies an inherent power to conduct warrantless searches. In 1995, we justified warrantless national security searches by recognizing that the executive branch needed flexibility in conducting foreign intelligence operations. Memorandum for Michael Vatis, Deputy Director, Executive Office for National Security, from Walter Dellinger, Assistant Attorney General, *Re: Standards for Searches Under Foreign Intelligence Surveillance Act* (Feb. 14, 1995). In 1980, we also said that "the lower courts – as well as this Department – have frequently concluded that authority does exist in the President to authorize such searches regardless of whether the courts also have the power to issue warrants for those searches. Memorandum for the Attorney General, from John M. Harmon, Assistant Attorney General, *Re: Inherent Authority* at 1 (Oct. 10, 1980).[2] FISA cannot infringe the President's inherent power under the Constitution to conduct national security searches, just as Congress cannot enact legislation that would interfere with the President's Commander-in-Chief power to conduct military hostilities. In either case, congressional efforts to regulate the exercise of an inherent executive power would violate the separation of powers by allowing the legislative branch to usurp the powers of the executive. *See* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001) (War Powers Resolution cannot constitutionally define or regulate the President's Commander-in-Chief authority). Indeed, as we will see in Part IV, the Fourth Amendment's structure and Supreme Court case law demonstrate that the executive may engage in warrantless searches so long as the search is reasonable.

The federal courts have recognized the President's constitutional authority to conduct warrantless searches for national security purposes. To be sure, the Supreme Court has held that the warrant requirement should apply in cases of terrorism by purely domestic groups, *see United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 299 (1972) ("*Keith*"), and has explicitly has not reached the scope of the President's surveillance powers with respect to the activities of foreign powers, *id.* at 308; *see also Katz. v. United States*, 389 U.S. 347, 358 n.23 (1967); *Mitchell*

---

[1]A short description of this history is attached to this letter.

[2]Based on similar reasoning, this Office has concluded that the President could receive materials, for national defense purposes, acquired through Title III surveillance methods or grand juries. Memorandum for Frances Fragos Townsend, Counsel, Office of Intelligence Policy and Review, from Randolph D. Moss, Assistant Attorney General, *Re: Title III Electronic Surveillance Material and the Intelligence Community* (Oct. 17, 2000); Memorandum for Gerald A. Schroeder, Acting Counsel, Office of Intelligence Policy and Review, from Richard L. Shiffrin, Deputy Assistant Attorney General, *Re: Grand Jury Material and the Intelligence Community* (Aug. 14, 1997); *Disclosure of Grand Jury Matters to the President and Other Officials*, 17 Op. O.L.C. 59 (1993).

v. Forsyth, 472 U.S. 511, 531 (1985). Nevertheless, even after *Keith* the lower courts have continued to find that when the government conducts a search for national security reasons, of a foreign power or its agents, it need not meet the same requirements that would normally apply in the context of criminal law enforcement, such as obtaining a judicial warrant pursuant to a showing of probable cause. *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); *United States v. Buck*, 548 F.2d 871 (9th Cir.), *cert. denied* 434 U.S. 890 (1977); *United States v. Butenko*, 494 F.2d 593 (en banc), *cert. denied*, 419 U.S. 881 (1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971). Indeed, even FISA – which does not require a showing of probable cause – represents congressional agreement with the notion that surveillance conducted for national security purposes is not subject to the same Fourth Amendment standards that apply in domestic criminal cases.

Truong Dinh Hung exemplifies the considerations that have led the federal courts to recognize the President's constitutional authority to conduct warrantless national security searches. Unlike the domestic law enforcement context, the President's enhanced constitutional authority in national security and foreign affairs justifies a freer hand in conducting searches without ex ante judicial oversight. As the Fourth Circuit found, "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . 'unduly frustrate' the President in carrying out his foreign affairs responsibilities." *Truong Dinh Hung*, 629 F.2d at 913. A warrant requirement would be inappropriate, the court observed, because it would limit the executive branch's flexibility in foreign intelligence, delay responses to foreign intelligence threats, and create the chance for leaks. *Id.* Further, in the area of foreign intelligence, the executive branch is paramount in its expertise and knowledge, while the courts would have little competence in reviewing the government's need for the intelligence information. *Id.* at 913-14. In order to protect individual privacy interests, however, the court limited the national security exception to the warrant requirement to cases in which the object of the search is a foreign power, its agents, or collaborators, and when the surveillance is conducted primarily for foreign intelligence reasons. *Id.* at 915. The other lower courts to have considered this question similarly have limited the scope of warrantless national security searches to those circumstances.

Here, it seems clear that the current environment falls within the exception to the warrant requirement for national security searches. Foreign terrorists have succeeded in launching a direct attack on important military and civilian targets within the United States. The President may find that terrorists constitute an ongoing threat against the people of the United States and their national government, and he may find that protecting against this threat is a compelling government interest. The government would be conducting warrantless searches in order to discover information that will prevent future attacks on the United States and its citizens. This surveillance may provide information on the strength of terrorist groups, the timing and methods of their attack, and the target. The fact that the foreign terrorists have operated, and may continue to operate, within the domestic United States, does not clothe their operations in the constitutional protections that apply to domestic criminal investigations. See Memorandum for Alberto R.

Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: *Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While some information might prove useful to law enforcement, the purpose of the surveillance program remains that of protecting the national security. As we have advised in a separate memorandum, a secondary law enforcement use of information, which was originally gathered for national security purposes, does not suddenly render the search subject to the ordinary Fourth Amendment standards that govern domestic criminal investigations. *See* Memorandum for David S. Kris, Associate Deputy Attorney General, from John C. Yoo, Deputy Assistant Attorney General, *Re: Constitutionality of Amending Foreign Intelligence Surveillance Act to Change the "Purpose" Standard for Searches* (Sept. 25, 2001).

Due to the President's paramount constitutional authority in the field of national security, a subject which we will discuss in more detail below, reading FISA to prohibit the President from retaining the power to engage in warrantless national security searches would raise the most severe of constitutional conflicts. Generally, courts will construe statutes to avoid such constitutional problems, on the assumption that Congress does not wish to violate the Constitution, unless a statute clearly demands a different construction. *See, e.g., Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Unless Congress signals a clear intention otherwise, a statute must be read to preserve the President's inherent constitutional power, so as to avoid any potential constitutional problems. *Cf. Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989) (construing Federal Advisory Committee Act to avoid unconstitutional infringement on executive powers); *Association of American Physicians & Surgeons v. Clinton*, 997 F.2d 898, 906-11 (D.C. Cir. 1993) (same). Thus, unless Congress made a clear statement in FISA that it sought to restrict presidential authority to conduct warrantless searches in the national security area – which it has not – then the statute must be construed to avoid such a reading. Even if FISA's liability provisions were thought to apply, we also believe that for a variety of reasons they could not be enforced against surveillance conducted on direct presidential order to defend the nation from attack. This issue can be discussed in more detail, if desired.

III.

Having established that the President has the authority to order the conduct of electronic surveillance without a warrant for national security purposes, we now examine the justification under the Fourth Amendment for the specific searches that might arise. The Fourth Amendment declares that "the right of the people to be secure in their persons, houses, papers, and effects, against *unreasonable* searches and seizures, shall not be violated." U.S. Const. amend IV. The Amendment also declares that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *Id.* This Part will discuss the reasons why several elements of a possible surveillance program would not even trigger Fourth Amendment

scrutiny because they would not constitute a "search" for constitutional purposes.

A.

Aspects of surveillance that do not involve United States persons and that occur extraterritorially do not raise Fourth Amendment concerns. As the Supreme Court has found, the Fourth Amendment does not apply to military or intelligence operations conducted against aliens overseas. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). In *Verdugo-Urquidez*, the Court found that the purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters. *Id.* at 266. As the Court concluded, the Fourth Amendment's design was "to protect the people of the United States against arbitrary action by their own government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory." *Id.* Indeed, the Court reversed a court of appeals' holding that the Fourth Amendment applied extraterritorially because of its concern that such a rule would interfere with the nation's military operations abroad:

> The rule adopted by the Court of Appeals would apply not only to law enforcement operations abroad, but also to other foreign policy operations which might result in "searches or seizures." The United States frequently employs Armed Forces outside this country -- over 200 times in our history -- for the protection of American citizens or national security . . . . Application of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest. Were respondent to prevail, aliens with no attachment to this country might well bring actions for damages to remedy claimed violations of the Fourth Amendment in foreign countries or in international waters. . . . [T]he Court of Appeals' global view of [the Fourth Amendment's] applicability would plunge [the political branches] into a sea of uncertainty as to what might be reasonable in the way of searches and seizures conducted abroad.

Id. at 273-74 (citations omitted). Here, the Court made clear that aliens had no Fourth Amendment rights to challenge activity by the United States conducted abroad.

Thus, as applied, elements of a surveillance program would not even raise Fourth Amendment concerns, because much of the communications that the NSA would intercept would be those of non-U.S. persons abroad. [redacted] for example, which B1 B3 themselves do not terminate or originate in the United States and do not involve a U.S. person, do not involve a "search or seizure" under the Fourth Amendment. Further, any communications between terrorists that occur wholly abroad, and in which none of the terrorist participants are U.S. persons, also do not trigger Fourth Amendment scrutiny. An even narrower program, which would limit the interception

of communications involving terrorists to those that originate or terminate outside the United States, further narrows the likelihood that communications between U.S. persons within the United States will be intercepted.

B.

Second, intercepting certain communications that move internationally may not raise a Fourth Amendment issue because of what is known as the "border search exception." A surveillance program could direct the interception of all communications to or from another country in which terrorists are operating, which by definition would be international communication. Therefore, much if not all of the communications to be intercepted would cross the borders of the United States.

Under the border search exception to the Fourth Amendment, the federal government has the constitutional authority to search anything or anyone crossing the borders of the United States without violating any individual rights. In *United States v. Ramsey*, 431 U.S. 606 (1977), the Supreme Court upheld the constitutionality of searching incoming international mail based on reasonable cause to suspect that such mail contained illegally imported merchandise. Recognizing what it characterized as a "border search exception" to the Fourth Amendment's warrant and probable cause requirements, the Court observed that "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Id.* at 616. The Court made clear that the manner in which something or someone crossed the border made no difference. "It is clear that there is nothing in the rationale behind the border search exception which suggests that the mode of entry will be critical." *Id.* at 620. The Court also observed that there was no distinction to be drawn in what crossed the border; "[i]t is their entry into this country from without it that makes a resulting search 'reasonable.'" *Id.* Although the Supreme Court has not examined the issue, the lower courts have unanimously found that the border search exception also applies to the exit search of outgoing traffic as well.[3]

Based on this doctrine, the interception of international communications could be justified by analogizing to the border search of international mail. Although electronic mail is, in some sense, intangible, it is also a message that begins at a physical server computer and then, though the movement of digital signals across wires, is transmitted to another server computer in a different location. Electronic mail is just

---

[3]*See, e.g., United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995); *United States v. Berisha*, 925 F.2d 791 (5th Cir. 1991); *United States v. Ezeiruaku*, 936 F.2d 136 (3d Cir. 1991); *United States v. Nates*, 831 F.2d 860 (9th Cir. 1987), *cert. denied*, 487 U.S. 1205 (1988); *United States v. Hernandez-Salazar*, 813 F.2d 1126 (11th Cir. 1987); *United States v. Benevento*, 836 F.2d 60 (2d Cir. 1987), *cert. denied*, 486 U.S. 1043 (1988); *United States v. Udofot*, 711 F.2d 831 (8th Cir.), *cert. denied*, 464 U.S. 896 (1983).

a different method of transporting a communication across the border of the United States. As the Court emphasized in *Ramsey*, "[t]he critical fact is that the envelopes cross the border and enter this country, not that they are brought in by one mode of transportation rather than another." *Id.* at 620. The fact that the method of transportation is electronic, rather than physical, should not make a difference, nor should it matter that the search does not occur precisely when the message crosses the nation's borders. Indeed, searches of outbound or inbound international mail or luggage take place at facilities within the nation's borders, after they have arrived by air, just as searches of electronic messages could occur once an international message appears on a server within the United States after transmission across our borders. It should be admitted that we have not found any cases applying *Ramsey* in this manner, although we also have not found any reported cases in which a court was confronted with a search effort of all international communications either.

There are three further caveats to raise in regard to the border search exception theory. First, it is altogether unclear whether *Ramsey* would apply at all to telephone conversations. While telephone conversations are like letters in that they convey messages, they are also ongoing, real-time transactions which do not contain discrete, self-contained chunks of communication. Second, and related to the first point, the Court has cautioned that examination of international mail for its content would raise serious constitutional questions. In *Ramsey*, the government opened outgoing mail that it suspected contained illegal drugs; regulations specifically forbade customs officials from reading any correspondence. Thus, the crime there was not the content of the communication itself, although the content could have been related to the transportation of the illegal substance. First Amendment issues would be raised if the very purpose of opening correspondence was to examine its content. *Id.* at 623-24. Third, the Court observed that serious constitutional problems in *Ramsey* were avoided due to a probable cause requirement. While this Office has advised that a reasonableness standard might still be constitutional if applied to international mail searches, we also acknowledged that our conclusion was not free from doubt. *See* Memorandum for Geoffrey R. Greiveldinger, Counsel for National Security Matters, Criminal Division, from Teresa Wynn Roseborough and Richard L. Shiffrin, Deputy Assistant Attorneys General, *Customs Service Proposal for Outbound Mail Search Authority, Amendment of Titles 31 U.S.C. § 5317(b) and 39 U.S.C. § 3623(d)* (Oct. 31, 1995). In light of these caveats, we can conclude that the border search exception would apply most squarely to the acquisition of communication addressing information, which for reasons we discuss below is not content, but might not reach the interception of the contents of telephone or other electronic communication.

C.

Third, the interception of electronic mail for its non-content information should not raise Fourth Amendment concerns. Capturing only the non-content addressing information of electronic communications may be analogized to a "pen register." A pen register is a device that records the numbers dialed from a telephone. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court found that the

warrantless installation of a pen register for a defendant's home phone line did not violate the Fourth Amendment because use of a pen register was not a "search" within the meaning of the Amendment. Applying the test set out in *Katz v. United States*, 389 U.S. 347 (1967), the Court evaluated whether a person could claim a "legitimate expectation of privacy" in the phone numbers dialed. It found that a person could not have a legitimate expectation of privacy, because they should know that they numbers dialed are recorded by the phone company for legitimate business purposes, and that a reasonable person could not expect that the numerical information he voluntarily conveyed to the phone company would not be "exposed." *Id.* at 741-46. Because pen registers do not acquire the contents of communication, and because a person has no legitimate expectation of privacy in the numbers dialed, the Court concluded, use of a pen register does not constitute a search for Fourth Amendment purposes.

The Court's blessing of pen registers suggests that a surveillance program that sought only non-content information from electronic messages would be similarly constitutional. An interception program for electronic mail, for example, could capture only non-content information in regard to which a reasonable person might not have a legitimate expectation of privacy. E-mail addresses, like phone numbers, are voluntarily provided by the sender to the internet service provider (ISP) in order to allow the company to properly route the communication. A reasonable person could be expected to know that an ISP would record such message information for their own business purposes, just as telephone companies record phone numbers dialed. Furthermore, other information such as routing and server information is not even part of the content of a message written by the sender. Rather, such information is generated by the ISP itself, as part of its routine business operations, to help it send the electronic message through its network to the correct recipient. A sender could have no legitimate expectation of privacy over information he did not even include in his message, but instead is created by the ISP as part of its own business processes. A person would have no more privacy interest in that information than he would have in a postmark stamped onto the outside of an envelope containing his letter.

Whether a surveillance program involving electronic mail would sweep in content poses a more difficult question. From *Smith,* it appears that a pen register does not effectuate a Fourth Amendment search, in part, because it does not capture content from a communication. "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed." *Smith*, 442 U.S. at 741. Here, it is no doubt true that electronic mail addressing information, created by the author of a communication, could contain some content. Variations of an addressee's name are commonly used to create e-mail addresses, and elements of the address can reveal other information, such as the institution or place someone works – hence, my e-mail address, assigned to me by the Justice Department, is john.c.yoo@usdoj.gov. This, however, does not render such information wholly subject to the Fourth Amendment. Even phone numbers can provide information that contains content. Phone numbers, for example, are sometimes used to spell words (such as 1-800-CALL-ATT), phone numbers can provide some location information, such as if someone calls a well-known hotel's number, and keypunches can even send messages, such as through pager systems. We believe that an individual's willingness to convey

to an ISP addressing information, which the ISP then uses for its own business purposes, suggests that an individual has no legitimate expectation of privacy in the limited content that could be inferred from e-mail addresses. We also note, however, that the courts have yet to encounter this issue in any meaningful manner, and so we cannot predict with certainty whether the judiciary would agree with our approach.

It should be noted that Congress has recognized the analogy between electronic mail routing information and pen registers. It recently enacted legislation authorizing pen register orders for non-content information from electronic mail. See USA Patriot Act of 2001, Pub. L. No. 107-56, § 216. While Congress extended pen register authority to surveillance of electronic mail, it also subjected that authority to the general restrictions of Title III and FISA, which require the Justice Department to obtain an ex parte court order before using such devices. While the requirements for such an order are minimal, see 18 U.S.C. § 3122 (government attorney must certify only that information likely to be gained from pen register "is relevant to an ongoing criminal investigation being conducted by that agency"), a warrantless surveillance program would not seek a judicial order for the surveillance program here. Title III attempts to forbid the use of pen registers or, now, electronic mail trap and trace devices, without a court under Title III or FISA. *Id.* at § 3121(a). As with our analysis of FISA, however, we do not believe that Congress may restrict the President's inherent constitutional powers, which allow him to gather intelligence necessary to defend the nation from direct attack. *See supra*. In any event, Congress's belief that a court order is necessary before using a pen register does not affect the constitutional analysis under the Fourth Amendment, which remains that an individual has no Fourth Amendment right in addressing information. Indeed, the fact that use of pen register and electronic trap and trace devices can be authorized without a showing of probable cause demonstrates that Congress agrees that such information is without constitutional protections.

D.

Fourth, intelligence gathering in direct support of military operations does not trigger constitutional rights against illegal searches and seizures. Our Office has recently undertaken a detailed examination of whether the use of the military domestically in order to combat terrorism would be restricted by the Fourth Amendment. *See* Memorandum for Alberto R. Gonzalez, Counsel to the President and William J. Haynes, II, General Counsel, Department of Defense, from John C. Yoo, Deputy Assistant Attorney General and Robert J. Delahunty, Special Counsel, Re: *Authority for Use of Military Force to Combat Terrorist Activities Within the United States* (Oct. 23, 2001). While we will only summarize here our reasoning, it should be clear that to the extent that a surveillance program is aimed at gathering intelligence for the military purpose of using the Armed Forces to prevent further attacks on the United States, that activity in our view is not restricted by the Fourth Amendment.

As a matter of the original understanding, the Fourth Amendment was aimed primarily at curbing law enforcement abuses. Although the Fourth Amendment has been interpreted to apply to governmental actions other than criminal law enforcement, the central concerns of the Amendment are focused on police

activity. *See, e.g., South Dakota v. Opperman*, 428 U.S. 364, 370 n.5 (1976). As we will explain in further detail in Part IV below, the Court has recognized this by identifying a "special needs" exception to the Fourth Amendment's warrant and probable cause requirements. *See, e.g., Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995); *Indianapolis v. Edmond*, 531 U.S. 32 (2000). However well suited the warrant and probable cause requirements may be as applied to criminal investigation and law enforcement, they are unsuited to the demands of wartime and the military necessity to successfully prosecute a war against an enemy. In the circumstances created by the September 11 attacks, the Constitution provides the Government with expanded powers and reduces the restrictions created by individual civil liberties. As the Supreme Court has held, for example, in wartime the government may summarily requisition property, seize enemy property, and "even the personal liberty of the citizen may be temporarily restrained as a measure of public safety." *Yakus v. United States*, 321 U.S. 414, 443 (1944) (citations omitted). "In times of war or insurrection, when society's interest is at its peak, the Government may detain individuals whom the Government believes to be dangerous." *United States v. Salerno*, 481 U.S. 739, 748 (1987); *see also Moyer v. Peabody*, 212 U.S. 78 (1909) (upholding detention without probable cause during time of insurrection) (Holmes, J.).

Because of the exigencies of war and military necessity, the Fourth Amendment should not be read as applying to military operations. In *Verdugo-Urquidez*, discussed in Part III, the Court made clear that the Fourth Amendment does not apply to military operations overseas. 494 U.S. at 273-274. As the Court observed, if things were otherwise, both political leaders and military commanders would be severely constrained by having to assess the "reasonableness" of any military action beforehand, thereby interfering with military effectiveness and the President's constitutional responsibilities as Commander-in-Chief. It also seems clear that the Fourth Amendment would not restrict military operations within the United States against an invasion or rebellion. *See, e.g.*, 24 Op. Att'y Gen. 570 (1903) (American territory held by enemy forces is considered hostile territory where civil laws do not apply). Were the United States homeland invaded by foreign military forces, our armed forces would have to take whatever steps necessary to repel them, which would include the "seizure" of enemy personnel and the "search" of enemy papers and messages, it is difficult to believe that our government would need to show that these actions were "reasonable" under the Fourth Amendment. The actions of our military, which might cause collateral damage to United States persons, would no more be constrained by the Fourth Amendment than if their operations occurred overseas. Nor is it necessary that the military forces on our soil be foreign. Even if the enemies of the Nation came from within, such as occurred during the Civil War, the federal Armed Forces must be free to use force to respond to such an insurrection or rebellion without the constraints of the Fourth Amendment. Indeed, this was the understanding that prevailed during the Civil War.

These considerations could justify much of a warrantless electronic surveillance program. Although the terrorists who staged the September 11, 2001 events operated clandestinely and have not occupied part of our territory, they have launched a direct attack on both the American homeland and our assets overseas that have caused massive casualties. Their attacks were launched and carried out from within the

United States itself. Pursuant to his authority as Commander-in-Chief and Chief Executive, the President has ordered the use of military force against the terrorists both at home and abroad, and he has found that they present a continuing threat of further attacks on the United States. Application of the Fourth Amendment could, in many cases, prevent the President from fulfilling his highest constitutional duty of protecting and preserving the Nation from direct attack. Indeed, the opposite rule would create the bizarre situation in which the President would encounter less constitutional freedom in using the military when the Nation is directly attacked at home, where the greatest threat to American civilian casualties lies, than we use force abroad.

Thus, the Fourth Amendment should not limit military operations to prevent attacks that take place within the American homeland, just as it would not limit the President's power to respond to attacks launched abroad. A surveillance program, undertaken for national security purposes, would be a necessary element in the effective exercise of the President's authority to prosecute the current war successfully. Intelligence gathered through surveillance allows the Commander-in-Chief to determine how best to position and deploy the Armed Forces. It seems clear that the primary purpose of the surveillance program is to defend the national security, rather than for law enforcement purposes, which might trigger Fourth Amendment concerns. In this respect, it is significant that the President would be ordering the Secretary of Defense (who supervises the NSA), rather than the Justice Department, to conduct the surveillance, and that evidence would not be preserved for later use in criminal investigations. While such secondary use of such information for law enforcement does not undermine the primary national security purpose motivating the surveillance program, it is also clear that such intelligence material, once developed, can be made available to the Justice Department for domestic use.

IV.

Even if a surveillance program, or elements of it, were still thought to be subject to Fourth Amendment scrutiny, we think that compelling arguments can justify its constitutionality. This Part will review whether warrantless electronic surveillance, undertaken for national security purposes, is constitutional under the Fourth Amendment. It should be clear at the outset that the Fourth Amendment does not require a warrant for every search, but rather that a search be "reasonable" to be constitutional. In light of the current security environment, the government can claim a compelling interest in protecting the nation from attack sufficient to outweigh any intrusion into privacy interests.

A.

The touchstone for review of a government search is whether it is "reasonable." According to the Supreme Court, "[a]s the text of the Fourth Amendment indicates the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995). When law enforcement undertakes a search to discover evidence of criminal

wrongdoing, the Supreme Court has said that reasonableness generally requires a judicial warrant on a showing of probable cause that a crime has been or is being committed. *Id.* at 653. But the Court has also recognized that a warrant is not required for all government searches, especially those that fall outside the ordinary criminal investigation context. A warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Id.*

A variety of government searches, therefore, have met the Fourth Amendment's requirement of reasonableness without obtaining a judicial warrant. The Supreme Court, for example, has upheld warrantless searches that involved the drug testing of high school athletes, *id.*, certain searches of automobiles, *Pennsylvania v. Labron*, 518 U.S. 938 (1996) (per curiam), drunk driver checkpoints, *Michigan v. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990), drug testing of railroad personnel, *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989), drug testing of federal customs officers, *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989), administrative inspection of closely regulated businesses, *New York v. Burger*, 482 U.S. 691 (1987); temporary baggage seizures, *United States v. Place*, 462 U.S. 696 (1983), detention to prevent flight and to protect law enforcement officers, *Michigan v. Summers*, 452 U.S. 692 (1981), checkpoints to search for illegal aliens, *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), and temporary stops and limited searches for weapons, *Terry v. Ohio*, 392 U.S. 1 (1968). The Court has cautioned, however, that a random search program cannot be designed to promote a general interest in crime control. *See Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000); *Delaware v. Prouse*, 440 U.S. 648, 659 n.18 (1979).

Reasonableness does not lend itself to precise tests or formulations. Nonetheless, in reviewing warrantless search programs, the Court generally has balanced the government's interest against intrusion into privacy interests. "When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *Illinois v. McArthur*, 121 S. Ct. 946, 949 (2001). Or, as the Court has described it, warrantless searches may be justified if the government has "special needs" that are unrelated to normal law enforcement. In these situations, the Court has found a search reasonable when, under the totality of the circumstances, the "importance of the governmental interests" has outweighed the "nature and quality of the intrusion on the individual's Fourth Amendment interests." *Tennessee v. Garner*, 471 U.S. 1, 8 (1985).

B.

This analysis suggests that the Fourth Amendment would permit warrantless electronic surveillance if the government's interest outweighs intrusions into privacy interests. It should be clear that the President's directive falls within the "special needs" exception to the warrant requirement that calls for such a balancing test. The surveillance program is not designed to advance a "general interest in crime control,"

Edmond, 531 U.S. at 44, but instead seeks to protect the national security by preventing terrorist attacks upon the United States. As the national security search cases discussed in Part II recognize, defending the nation from foreign threats is a wholly different enterprise than ordinary crime control, and this difference justifies examination of the government's action solely for its reasonableness. Indeed, as the Supreme Court recognized in *Edmond*, warrantless, random searches undertaken for national security purposes, such as forestalling a terrorist attack on an American city, would be constitutional even if the same search technique, when undertaken for general crime control, would fail Fourth Amendment standards.

Applying this standard, we find that the government's interest here is perhaps of the highest order – that of protecting the nation from attack. Indeed, the factors justifying warrantless searches for national security reasons are more compelling now than at the time of the earlier lower court decisions discussed in Part II. While upholding warrantless searches for national security purposes, those earlier decisions had not taken place during a time of actual hostilities prompted by a surprise, direct attack upon civilian and military targets within the United States. A direct attack on the United States has placed the Nation in a state of armed conflict; defending the nation is perhaps the most important function of government. As the Supreme Court has observed, "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). As Alexander Hamilton observed in *The Federalist*, "there can be no limitation of that authority, which is to provide for the defence and protection of the community, in any matter essential to its efficacy." *The Federalist* No. 23, at 147-48 (Alexander Hamilton) (Jacob E. Cooke ed., 1961). If the situation warrants, the Constitution recognizes that the federal government, and indeed the President, must have the maximum power permissible under the Constitution to prevent and defeat attacks upon the Nation.

In authorizing an electronic surveillance program, the President should lay out the proper factual predicates for finding that the terrorist attacks had created a compelling governmental interest. The September 11, 2001 attacks caused thousands of deaths and even more casualties, and damaged both the central command and control facility for the Nation's military establishment and the center of the country's private financial system. In light of information that would be provided by the intelligence community and the military, the President could further conclude that terrorists continue to have the ability and the intention to undertake further attacks on the United States. Given the damage caused by the attacks on September 11, 2001, the President could judge that future terrorist attacks could cause massive damage and casualties and threatens the continuity of the federal government. He could conclude that such circumstances justify a compelling interest on the part of the government to protect the United States and its citizens from further terrorist attack. It seems certain that the federal courts would defer to the President's determination on whether the United States is threatened by attack and what measures are necessary to respond. *See, e.g., The Prize Cases,* 67 U.S. 635, 670 (1862) (decision whether to consider rebellion a war is a question to be decided by the President). These determinations rest at the core of the President's power as Commander-in-Chief and his role as representative of the Nation in its foreign affairs. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304 (1936).

Under the Constitution's design, it is the President who is primarily responsible for advancing that compelling interest. The text, structure, and history of the Constitution establish that the President bears the constitutional duty, and therefore the power, to ensure the security of the United States in situations of grave and unforeseen emergency. *See generally* Memorandum for Timothy E. Flanigan, Deputy Counsel to the President, from John C. Yoo, Deputy Assistant Attorney General, *Re: The President's Constitutional Authority to Conduct Military Operations Against Terrorists and Nations Supporting Them* (Sept. 25, 2001). Both the Vesting Clause, U.S. Const. art. II, § 1, cl. 1, and the Commander in Chief Clause, *id.*, § 2, cl. 1, vest in the President the power to deploy military force in the defense of the United States. The Constitution makes explicit the President's obligation to safeguard the nation's security by whatever lawful means are available by imposing on him the duty to "take Care that the Laws be faithfully executed." *Id.*, § 3. The constitutional text and structure are confirmed by the practical consideration that national security decisions require a unity in purpose and energy in action that characterize the Presidency rather than Congress. As Alexander Hamilton explained, "[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand." *The Federalist* No. 74, at 500 (Alexander Hamilton) (Jacob E. Cooke ed. 1961).

Surveillance initiated in response to the September 11 attacks would clearly advance this interest. The President would be exercising his powers as Commander-in-Chief and Chief Executive to direct military action against Al Qaeda and Taliban forces in Afghanistan, and to use the armed forces to protect United States citizens at home. Congress has approved the use of military force in response to the September 11 attacks. Pub. L. No. 107-40, 115 Stat. 224 (2001). It is well established that the President has the independent constitutional authority as Commander-in-Chief to gather intelligence in support of military and national security operations, and to employ covert means, if necessary, to do so. *See Totten v. United States*, 92 U.S. 105, 106 (1876). The President's "constitutional power to gather foreign intelligence," *Warrantless Foreign Intelligence Surveillance – Use of Television – Beepers*, 2 Op. O.L.C. 14, 15 (1978), includes the discretion to use the most effective means of obtaining information, and to safeguard those means. Intelligence gathering is a necessary function that enables the President to carry out these authorities effectively. The Commander-in-Chief needs accurate and comprehensive intelligence on enemy movements, plans, and threats in order to best deploy the United States armed forces and to successfully execute military plans. Warrantless searches could provide the most effective method, in the President's judgment, to obtain information necessary for him to carry out his constitutional responsibility to defend the Nation from attack.

By contrast, the intrusion into an individual citizen's privacy interests may not be seen as so serious as outweighing the government's most compelling of interests. The searches that would take place are as not as intrusive as those which occur when the government monitors the communications of a target in the normal Title III or FISA context. These often require an agent to consciously and actively listen in to telephone conversations. Here, as we understand it, [redacted] B1 B3

B1
B3

[redacted]

If privacy interests are viewed as intruded upon only by [redacted] it is likely that Fourth Amendment interests would not outweigh the compelling governmental interest present here. In the context of roadblocks to stop drunken drivers, another area of "special needs" under the Fourth Amendment, the Court has permitted warrantless searches. *See Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990). There, the Court found that a roadblock constituted a "reasonable" search due to the magnitude of the drunken driver problem and the deaths it causes – in fact, the court compared the death toll from drunk drivers to the casualties on a battlefield. *Id.* at 451. It found that this interest outweighed the intrusion into privacy at a checkpoint stop, which it characterized as "brief" in terms of duration and intensity. Similarly, [redacted] than in the case of a roadblock, where a [redacted] law enforcement officer stops each driver to examine whether they are inebriated. It seems that if the Supreme Court were willing to uphold drunk driver checkpoints, it would be equally or even more willing to allow [redacted][4]

B1
B3

B1
B3

B1
B3

The restriction of a surveillance program only to those communications which originate or terminate in a foreign country or which involve terrorists further reduces any possible intrusion into individual privacy interests. If probable cause is required, it seems that DOD would need specific evidence before deciding which messages to intercept. Thus, for example, DOD must have some information that a certain person might be a terrorist, or that a certain phone line might be used by a terrorist, before it can capture the communications. This means that the NSA cannot intercept communications for which it has no such evidence. This would be the case even if the President were to require that there be reasonable grounds to believe that the communications involve the relevant foreign country or terrorists. This has the effect of excluding communications for which DOD has no reason to suspect contain terrorist communications or communications with the foreign country, meaning that most innocent communications will not be

---

[4]Another factor examined by the Court was effectiveness of the warrantless search. The Court has cautioned that searches not be random and discretionless because of a lack of empirical evidence that the means would promote the government's interest. It should be made clear, however, that the standard employed by the Court has been low. In the roadblock context, for example, the Court has found reasonable roadblocks for drunk drivers that detained only 1.6 percent of all drivers stopped, and checkpoints for illegal aliens that detained only 0.12 percent of all vehicles detained.

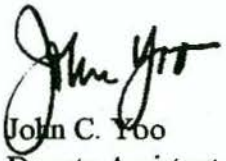
intercepted.

Further, limiting the search parameters to international communications could further alleviate any intrusion into individual privacy interests. As our discussion of the border search exception in Part III made clear, the government has the constitutional authority to search anything that crosses the Nation's borders without violating the Fourth Amendment. To be sure, there is substantial doubt about whether this power could apply to searches involving the content of the communications. Nonetheless, *United States v. Ramsey*, 431 U.S. 606 (1977) (warrantless search of incoming international mail does not violate Fourth Amendment), suggests strongly that individuals have reduced privacy interests when they or their possessions and letters cross the borders of the United States. If individuals have reduced privacy interests in international mail, as *Ramsey* held, then it seems logical to assume that they also have a reduced privacy interest in international electronic communications as well. As *Ramsey* held, the method by which an item entered the country is irrelevant for Fourth Amendment purposes.

Just to be clear in conclusion. We are not claiming that the government has an unrestricted right to examine the contents of all international letters and other forms of communication. Rather, we are only suggesting that an individual has a reduced privacy interest in international communications Therefore, in applying the balancing test called for by the Fourth Amendment's reasonableness analysis, we face a situation here where the government's interest on one side – that of protecting the Nation from direct attack – is the highest known to the Constitution. On the other side of the scale, the intrusion into individual privacy interests is greatly reduced due to the international nature of the communications. Thus, we believe there to be substantial justification for a warrantless electronic surveillance program, undertaken in response to the September 11, 2001 attacks, that would be reasonable under the Fourth Amendment.

I would welcome the opportunity to discuss these issues in more detail. Please contact me, at 202-514-2069, or john.c.yoo@usdoj.gov, if you have any further questions.

Sincerely,



John C. Yoo
Deputy Assistant Attorney General

AUTHORITY FOR WARRANTLESS NATIONAL SECURITY SEARCHES

Presidents have long asserted the constitutional authority to order searches, even without judicial warrants, where necessary to protect the national security against foreign powers and their agents. The courts have repeatedly upheld the exercise of this authority.

A memorandum from President Franklin D. Roosevelt to Attorney General Robert H. Jackson, dated May 21, 1940, authorized the use of wiretaps in matters "involving the defense of the nation." *See United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 311 n.10 (1972) ("*Keith*"). The President directed the Attorney General "to secure information by listening devices [directed at] the conversation or other communications of persons suspected of subversive activities against the government of the United States, including suspected spies," while asking the Attorney General "to limit these investigations so conducted to a minimum and to limit them insofar as possible as to aliens." *See* Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings Before the Subcomm. on Intelligence and the Rights of Americans of the Select Comm. on Intelligence, 94th Cong., 2d Sess. 24 (1976) (statement of Attorney General Edward H. Levi) ("Levi Statement"). President Roosevelt issued the memorandum after the House of Representatives passed a joint resolution to sanction wiretapping by the FBI for national security purposes, but the Senate failed to act. *See* Americo R. Cinquegrana, *The Walls and Wires Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Pa. L. Rev. 793, 797-98 (1989).

By a letter dated July 17, 1946, Attorney General Tom C. Clark reminded President Truman of the 1940 directive, which had been followed by Attorneys General Jackson and Francis Biddle. At Attorney General Clark's request, the President approved the continuation of the authority, *see* Levi Statement at 24, and even broadened it to reach "internal security cases." *Keith*, 407 U.S. at 311 and n.10. In the Eisenhower Administration, Attorney General Herbert Brownell, as the Supreme Court noted in *Keith*, advocated the use electronic surveillance both in internal and international security matters. 407 U.S. at 311.

In 1965, President Johnson announced a policy under which warrantless wiretaps would be limited to national security matters. Levi Statement at 26. Attorney General Katzenbach then wrote that he saw "no need to curtail any such activities in the national security field." *Id.* Attorney General Richardson stated in 1973 that, to approve a warrantless surveillance, he would need to be convinced that it was necessary "(1) to protect the nation against actual or potential attack or other hostile acts of a foreign power, (2) to obtain foreign intelligence information deemed essential to the security of the United States, or (3) to protect national security information against foreign intelligence activities." *Id.* at 27. When Attorney General Levi testified in 1976, he gave a similar list, adding that a warrantless surveillance could also be used "to obtain information certified as necessary for the conduct of foreign

affairs matters important to the national security of the United States." *Id.*

Warrantless electronic surveillance of agents of foreign powers thus continued until the passage in 1978 of the Foreign Intelligence Surveillance Act, 18 U.S.C. §§ 1801-29. Although the Supreme Court never ruled on the legality of warrantless searches as to agents of foreign powers, *see Keith*, 407 U.S. at 321-22 (requiring a warrant in domestic security cases but reserving issue where a foreign power or its agents were involved), the courts of appeals repeatedly sustained the lawfulness of such searches. *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593, 606 (3d Cir. 1974); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971); *but see Zweibon v. Mitchell*, 516 F.2d 594, 651 (D.C. Cir. 1975) (dictum in plurality opinion). The Fourth Circuit held, for example, that "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." *Truong*, 629 F.2d at 914. As the court elaborated, "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy," and a "warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *Id.* at 913 (citations and footnote omitted). Furthermore, "the executive possesses unparalleled expertise to make the decisions whether to conduct foreign intelligence surveillance." *Id.* (citations omitted). And "[p]erhaps 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." *Id.* at 914 (citations omitted). In this pre-statutory context, two courts of appeals, the Fourth Circuit in *Truong* (*id.* at 915) and the Third Circuit in *Butenko* (494 F.2d at 606), would have limited the authority to instances where the primary purpose of the search was to obtain foreign intelligence."

The passage of FISA created an effective means for issuance of judicial orders for electronic surveillance in national security matters. Congress, however, had not given the Foreign Intelligence Surveillance Court the power to issue orders for physical searches. After nevertheless granting orders in three instances during the Carter Administration, the court ruled early in the Reagan Administration, as the Justice Department then argued, that it lacked jurisdiction to approve physical searches. *See* S. Rep. 103-296, at 36-37 (1994). Thus, physical searches after the ruling had to approved by the Attorney General without a judicial warrant. *Id.* at 37. In 1994, after the use of warrantless physical searches in the Aldrich Ames case, Congress concluded that "from the standpoint of protecting the constitutional rights of Americans, from the standpoint of bringing greater legal certainty to this area, from the standpoint of avoiding problems with future espionage prosecutions, and from the standpoint of protecting federal officers and employees from potential civil liability," *id.*, FISA should be amended to cover physical searches. *Id.* at 40.