U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 22, 2005

The Honorable Pat Roberts
Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Honorable John D. Rockefeller, IV
Vice Chairman
Senate Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Honorable Peter Hoekstra
Chairman
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Jane Harman
Ranking Minority Member
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairmen Roberts and Hoekstra, Vice Chairman Rockefeller, and Ranking Member Harman:

As you know, in response to unauthorized disclosures in the media, the President has described certain activities of the National Security Agency ("NSA") that he has authorized since shortly after September 11, 2001. As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President has made clear that he will use his constitutional and statutory authorities to protect the American people from further terrorist attacks, and the NSA activities the President described are part of that effort. Leaders of the Congress were briefed on these activities more than a dozen times.

The purpose of this letter is to provide an additional brief summary of the legal authority supporting the NSA activities described by the President.

As an initial matter, I emphasize a few points. The President stated that these activities are "crucial to our national security." The President further explained that "the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country." These critical national security activities remain classified. All United States laws and policies governing the protection and nondisclosure of national security information, including the information relating to the

activities described by the President, remain in full force and effect. The unauthorized disclosure of classified information violates federal criminal law. The Government may provide further classified briefings to the Congress on these activities in an appropriate manner. Any such briefings will be conducted in a manner that will not endanger national security.

Under Article II of the Constitution, including in his capacity as Commander in Chief, the President has the responsibility to protect the Nation from further attacks, and the Constitution gives him all necessary authority to fulfill that duty. *See, e.g.*, *Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) (stressing that if the Nation is invaded, "the President is not only authorized but bound to resist by force . . . . without waiting for any special legislative authority"); *Campbell v. Clinton*, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) ("[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected."); *id.* at 40 (Tatel, J., concurring). The Congress recognized this constitutional authority in the preamble to the Authorization for the Use of Military Force ("AUMF") of September 18, 2001, 115 Stat. 224 (2001) ("[T]he President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States."), and in the War Powers Resolution, *see* 50 U.S.C. § 1541(c) ("The constitutional powers of the President as Commander in Chief to introduce United States Armed Forces into hostilities[] . . . [extend to] a national emergency created by attack upon the United States, its territories or possessions, or its armed forces.").

This constitutional authority includes the 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 . . . ."). The Supreme Court has said that warrants are generally required in the context of purely *domestic* threats, but it expressly distinguished *foreign* threats. *See United States v. United States District Court*, 407 U.S. 297, 308 (1972). As Justice Byron White recognized almost 40 years ago, Presidents have long exercised the authority to conduct warrantless surveillance for national security purposes, and a warrant is unnecessary "if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Katz v. United States*, 389 U.S. 347, 363-64 (1967) (White, J., concurring).

The President's constitutional authority to direct the NSA to conduct the activities he described is supplemented by statutory authority under the AUMF. The AUMF authorizes 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 of September 11, 2001, . . . in order to prevent any future acts of international terrorism against the United States." § 2(a). The AUMF clearly contemplates action within the United States, *see also id.* pmbl. (the attacks of September 11 "render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad"). The AUMF cannot be read as limited to authorizing the use of force against Afghanistan, as some

have argued. Indeed, those who directly "committed" the attacks of September 11 resided in the United States for months before those attacks. The reality of the September 11 plot demonstrates that the authorization of force covers activities both on foreign soil and in America.

In *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), the Supreme Court addressed the scope of the AUMF. At least five Justices concluded that the AUMF authorized the President to detain a U.S. citizen in the United States because "detention to prevent a combatant's return to the battlefield is a fundamental incident of waging war" and is therefore included in the "necessary and appropriate force" authorized by the Congress. *Id.* at 518-19 (plurality opinion of O'Connor, J.); *see id.* at 587 (Thomas, J., dissenting). These five Justices concluded that the AUMF "clearly and unmistakably authorize[s]" the "fundamental incident[s] of waging war." *Id.* at 518-19 (plurality opinion); *see id.* at 587 (Thomas, J., dissenting).

Communications intelligence targeted at the enemy is a fundamental incident of the use of military force. Indeed, throughout history, signals intelligence has formed a critical part of waging war. In the Civil War, each side tapped the telegraph lines of the other. In the World Wars, the United States intercepted telegrams into and out of the country. The AUMF cannot be read to exclude this long-recognized and essential authority to conduct communications intelligence targeted at the enemy. We cannot fight a war blind. 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. Accordingly, the President's "authority is at its maximum." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635 (1952) (Jackson, J., concurring); *see Dames & Moore v. Regan*, 453 U.S. 654, 668 (1981); *cf. Youngstown*, 343 U.S. at 585 (noting the absence of a statute "from which [the asserted authority] c[ould] be fairly implied").

The President's authorization of targeted electronic surveillance by the NSA is also consistent with the Foreign Intelligence Surveillance Act ("FISA"). Section 2511(2)(f) of title 18 provides, as relevant here, that the procedures of FISA and two chapters of title 18 "shall be the exclusive means by which electronic surveillance . . . may be conducted." Section 109 of FISA, in turn, makes it unlawful to conduct electronic surveillance, "except as authorized by statute." 50 U.S.C. § 1809(a)(1). Importantly, section 109's exception for electronic surveillance "authorized by statute" is broad, especially considered in the context of surrounding provisions. *See* 18 U.S.C. § 2511(1) ("Except as otherwise specifically provided *in this chapter* any person who—(a) intentionally intercepts . . . any wire, oral, or electronic communication[] . . . shall be punished . . . .") (emphasis added); *id.* § 2511(2)(e) (providing a defense to liability to individuals "conduct[ing] electronic surveillance, . . . as authorized by *that Act [FISA]*") (emphasis added).

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). The AUMF satisfies section 109's requirement for statutory authorization of electronic surveillance, just as a majority of the Court in *Hamdi* concluded that it satisfies the requirement in 18 U.S.C. § 4001(a) that no U.S. citizen be detained by the United States "except pursuant to an Act of Congress." *See Hamdi*, 542

U.S. at 519 (explaining that "it is of no moment that the AUMF does not use specific language of detention"); *see id.* at 587 (Thomas, J., dissenting).

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. *See, e.g., Zadvydas v. Davis*, 533 U.S. 678, 689 (2001); *INS v. St. Cyr*, 533 U.S. 289, 300 (2001). 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.

The NSA activities described by the President are also consistent with the Fourth Amendment and the protection of civil liberties. The Fourth Amendment's "central requirement is one of reasonableness." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). For searches conducted in the course of ordinary criminal law enforcement, reasonableness generally requires securing a warrant. *See Bd. of Educ. v. Earls*, 536 U.S. 822, 828 (2002). Outside the ordinary criminal law enforcement context, however, the Supreme Court has, at times, dispensed with the warrant, instead adjudging the reasonableness of a search under the totality of the circumstances. *See United States v. Knights*, 534 U.S. 112, 118 (2001). In particular, the Supreme Court has long recognized that "special needs, beyond the normal need for law enforcement," can justify departure from the usual warrant requirement. *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995); *see also City of Indianapolis v. Edmond*, 531 U.S. 32, 41-42 (2000) (striking down checkpoint where "primary purpose was to detect evidence of ordinary criminal wrongdoing").

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the "special needs" exception to the warrant requirement. Foreign intelligence collection undertaken to prevent further devastating attacks on our Nation serves the highest government purpose through means other than traditional law enforcement. *See In re Sealed Case*, 310 F.3d at 745; *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (recognizing that the Fourth Amendment implications of foreign intelligence surveillance are far different from ordinary wiretapping, because they are not principally used for criminal prosecution).

Intercepting communications into and out of the United States of persons linked to al Qaeda in order to detect and prevent a catastrophic attack is clearly *reasonable*. Reasonableness is generally determined by "balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests." *Earls*, 536 U.S. at 829. There is undeniably an important and legitimate privacy interest at stake with respect to the activities described by the President. That must be balanced, however, against the Government's compelling interest in the security of the Nation, *see, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (citation and quotation marks omitted). The fact that the NSA activities are reviewed and

reauthorized approximately every 45 days to ensure that they continue to be necessary and appropriate further demonstrates the reasonableness of these activities.

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. Nevertheless, I want to stress that the United States makes full use of FISA to address the terrorist threat, and FISA has proven to be a very important tool, especially in longer-term investigations. In addition, the United States is constantly assessing all available legal options, taking full advantage of any developments in the law.

We hope this information is helpful.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General