



U.S. Department of Justice

Office of Legal Counsel

Washington, D.C. 20530

November 26, 2014

Stephen Braun
Associated Press, Washington Bureau
sbraun@ap.org

Re: FOIA Tracking No. FY15-010

Dear Mr. Braun:

This letter responds to your June 27, 2013 Freedom of Information Act ("FOIA") request to the Department of Justice's Office of Information Policy ("OIP") in which you sought records regarding "complaints filed during the period of January 1, 2007 to the present . . . concerning the use, sharing, retention, improper collection, over-collection and/or dissemination of telephone and/or internet data or other information from or about U.S. persons." OIP, in turn, routed your request to the Office of Professional Responsibility ("OPR"). In processing your request, OPR referred one document to the Office of Legal Counsel for our review and direct response to you. We received the referral on November 7, 2014, and it was assigned tracking number **FY15-010**.

We are releasing the referred document to you in full.

Sincerely,

A handwritten signature in black ink, reading "Paul P. Colborn".

Paul P. Colborn
Special Counsel

Enclosure

LEGAL AUTHORITY FOR THE RECENTLY DISCLOSED NSA ACTIVITIES

1. 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 9/11. 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. Leaders of Congress from both parties were briefed on these activities more than a dozen times.
2. The President has made clear that he will use his constitutional and statutory authorities to protect the American people from further terrorist attacks. The surveillance conducted here is at the heart of the need to protect the Nation from attacks on our soil, since it involves communications into or out of the United States of persons linked to al Qaeda.
3. 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, a point Congress recognized 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."
 - A. This constitutional authority includes the authority to order foreign intelligence surveillance within the U.S. without seeking a warrant, 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"); *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (collecting authorities). 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) ("*Keith*").
 - B. Presidents of both parties have *consistently asserted* the authority to conduct foreign intelligence surveillance without a warrant. At the time FISA was passed, President Carter's Attorney General stated explicitly that the President would interpret FISA not to interfere with the President's constitutional powers and responsibilities. Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess. 15 (1978) (testimony of Attorney General Griffin Bell). President Clinton's Deputy Attorney General, Jamie Gorelick, explained to the House Intelligence Committee that "[t]he Department of Justice believes, and the case law supports, that the President has inherent authority to conduct warrantless physical searches for foreign intelligence purposes, and that the President may, as has been done, delegate this authority to the Attorney General." (July 14, 1994).

- C. As Justice Byron White noted almost 40 years ago, "[w]iretapping to protect the security of the Nation has been authorized by successive Presidents." *Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring).
4. The President's constitutional authority to authorize the NSA activities is supplemented by statutory authority under the AUMF.
- A. 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 that occurred on 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 U.S., *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"); it is not limited to Afghanistan. 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.
- B. A majority of the Supreme Court has explained that the AUMF "clearly and unmistakably authorize[s]" the "fundamental incident[s] of waging war." *Hamdi v. Rumsfeld*, 542 U.S. 507, 519 (2004) (plurality opinion of O'Connor, J.); *see id.* at 587 (Thomas, J., dissenting).
- C. Communications intelligence targeted at the enemy is a fundamental incident of the use of military force; we cannot fight a war blind. 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 U.S. intercepted telegrams into and out of the country. The AUMF uses expansive language that plainly encompasses the long-recognized and essential authority to conduct traditional communications intelligence targeted at the enemy.
- D. 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).
5. The President's authorization of targeted electronic surveillance by the NSA is consistent with the Foreign Intelligence Surveillance Act ("FISA").
- A. Section 2511(2)(f) of title 18 provides that the procedures of FISA and two chapters of title 18 "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." Section 109 of FISA, in turn, makes it unlawful to conduct electronic surveillance to obtain the content of such international communications when intercepted on cables in the U.S., "except as authorized by statute." 50 U.S.C. 1809(a)(1).
- B. By expressly 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. The AUMF satisfies section 109's requirement for statutory authorization of electronic surveillance, just as a majority of the Court in *Hamdi* concluded that the AUMF 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 ("it is of no moment that the AUMF does not use specific language of detention"); see *id.* at 587 (Thomas, J., dissenting).

- C. Even if it were also plausible to read FISA to contemplate that a subsequent statutory authorization must come in the form of an amendment to FISA itself, established principles of statutory construction require interpreting FISA to allow the AUMF to authorize necessary signals intelligence, thereby avoiding an interpretation of FISA that would raise grave constitutional questions.
6. If FISA were applied to prevent or frustrate the President's ability to create an early warning system to detect and prevent al Qaeda plots against the U.S., that application of FISA would be unconstitutional. The Court of Review that supervises the FISA court recognized as much, "taking for granted that the President does have" the authority "to conduct warrantless searches to obtain foreign intelligence information," and concluding that "FISA could not encroach on the President's constitutional power." *In re Sealed Case*, 310 F.3d 717 (FISA Ct. of Review 2002).
7. The NSA activities described by the President are fully consistent with the Fourth Amendment and the protection of civil liberties.
- A. The touchstone of the Fourth Amendment is *reasonableness*.
 - B. The Supreme Court has long recognized that "special needs, beyond the normal need for law enforcement," will justify departure from the usual warrant requirement. *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). Courts have recognized that the Fourth Amendment implications of national security surveillance are far different from ordinary wiretapping, because they are not principally used for criminal prosecution. See, e.g., *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984). See also *Katz v. United States*, 389 U.S. 347, 363-64 (White, J., concurring) (warrants not required "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").
 - C. Intercepting calls into and out of the U.S. of persons linked to al Qaeda in order to detect and prevent a catastrophic attack is such a "special need" and is clearly *reasonable* for Fourth Amendment purposes, particularly in light of the fact that the NSA activities are reviewed and reauthorized approximately every 45 days to ensure that they continue to be necessary and appropriate.
8. FISA could not have provided the speed and agility required for the early warning detection system the President determined was necessary following 9/11.
- A. In any event, the United States makes use of FISA to address the terrorist threat as appropriate, and FISA has proven to be a very important tool, especially in longer-term investigations.

B. The United States is constantly assessing all available legal options, taking full advantage of any developments in the law.

9. 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.