Elwood, Courtney

From: David.Kris@timewarner.com
Sent: Tuesday, December 20, 2005 6:23 PM
To: Elwood, Courtney
Subject: If you can't show me yours . . .

Attachments: tmp.htm; NSA Program Questions (12-20-05).doc


tmp.htm (4 KB)


NSA Program Questions (12-20-0..

FOIA EXEMPTION b6

Courtney --

I haven't spoken to Senator Feinstein -- she was supposed to call me but hasn't yet -- but in the meantime I wrote the attached. It is a VERY rough cut -- done quickly, without the facts, and in part while playing with [redacted]. If you or others inside DOJ want to clear up my muddled thinking on any issue, of course I'd be happy to hear your views. I figured this might be a kind of stopgap measure pending your decision on whether to make public OLC's analysis. Thanks,

-- David

David S. Kris
Chief Ethics and Compliance Officer
Time Warner Inc.
NY Tel: 212-484-7803
DC Tel: 202-530-7877
NY & DC Fax: 212-202-4381
Mobile: 301-537-6547
E-Mail: <mailto:david.kris@timewarner.com> david.kris@timewarner.com
One Time Warner Center 800 Connecticut Avenue, NW
14th Floor Suite 1200
New York, NY 10019 Washington, DC 20006

(8)

As I see things, the statutory and constitutional validity of the NSA surveillance program turns on the answers to five questions. I've tried to sketch out some discussion of the answers to those questions below. This is still a very rough draft, and I would want to think a lot more before saying anything definitive.

1. Did NSA engage in "electronic surveillance" as defined in FISA?

The answer to this question is almost surely "Yes." The Attorney General described NSA's conduct as "electronic surveillance of a particular kind, and this would be intercepts of contents of communications where . . . one party to the communication is outside the United States." (12/19/05 briefing). Implicit in the Attorney General's statement is that one party to the communication is inside the United States, and FISA's definition of "electronic surveillance" includes "the acquisition . . . of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States," apart from hacker communications. 50 U.S.C. § 1801(f)(2). Other subsections of the definition could also come into play, particularly if the target of the surveillance is a United States person – e.g., a citizen or green-card holder. See 50 U.S.C. § 1801(f)(2). No one has disputed that whatever NSA is doing, it is "electronic surveillance" as defined in FISA.

2. Did Congress in 1978 intend FISA's procedures (or those in Title III) to be the "exclusive means" by which the President could conduct "electronic surveillance" as defined in FISA?

Here too, the answer seems to be "Yes." A provision of FISA that is now codified at 18 U.S.C. § 2511(2)(f) provides in relevant part that "procedures in . . . the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in [50 U.S.C. § 1801(f)] . . . may be conducted" (emphasis added). The language of this "exclusivity provision" as a whole could be clearer,[1] but when read in light of FISA's legislative history its meaning is hard to avoid. The House Intelligence Committee's 1978 report on FISA explains (at page 101) that, "despite any inherent power of the President to authorize warrantless electronic surveillances in the absence of legislation, by [enacting FISA and Title III] Congress will have legislated with regard to electronic surveillance in the United States, that legislation with its procedures and safeguards prohibit[s] the President, notwithstanding any inherent

[1] Section 2511(2)(f) now provides as follows: "Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."

powers, from violating the terms of that legislation."[2] Congress recognized that the Supreme Court might disagree, but the 1978 House-Senate Conference report expresses an intent "to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own Constitutional power minus any Constitutional power of Congress over the matter.' *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952)."[3]

3. What are the "procedures" in FISA to which the exclusivity provision refers?

This is a bit of a tricky question. FISA creates the Foreign Intelligence Surveillance Court (FISC) and gives it "jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter." 50 U.S.C. § 1803(a) (emphasis added). Thus, the "procedures" in question seem at a minimum to include those governing the FISC's review and approval of FISA applications, which are set forth in 50 U.S.C. §§ 1804 and 1805 (for electronic surveillance), and require, among other things, the government to assert and the FISC to find "probable cause" that the target of the surveillance is a foreign power or an agent of a foreign power. The "procedures" in FISA would also presumably include any other rules under which the statute specifically authorizes electronic surveillance – i.e., the four situations set out in FISA in which electronic surveillance may be conducted (at least temporarily) even without FISC approval: (1) surveillance of communications systems used exclusively by foreign powers where there is no substantial likelihood of acquiring a U.S. person's communications (50 U.S.C. § 1802); (2) emergencies (50 U.S.C. § 1805(f)); (3) training and testing (50 U.S.C. § 1805(g)); and (4) immediately following a declaration of war by Congress (50 U.S.C. § 1811). In short, the "procedures" to which the exclusivity provision refers appear to be those procedures in FISA under which electronic surveillance is specifically authorized.

There is an alternative reading under which FISA's "procedures" could include those of any other statute, beyond FISA itself, that authorizes electronic surveillance. FISA contains provisions that establish criminal and civil liability for persons who intentionally "engage[] in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. §§ 1809 and 1810 (emphasis added). If these civil and criminal provisions are part of the "procedures" in FISA to which the exclusivity provision refers, then perhaps the exclusivity provision permits electronic surveillance not only as specifically authorized by FISA itself, but also electronic surveillance as authorized by any statute, including statutes other than FISA (and Title III, which as noted above is specifically cited in the exclusivity provision). This reading is a stretch, in my view,

---

[2] *See also* FISA Senate Judiciary Report at 64 (FISA "puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in [Title III and FISA]"); FISA Senate Intelligence Report at 71 (same).

[3] FISA House Conference Report at 35.

because the civil and criminal penalty provisions in FISA are not really procedures for conducting electronic surveillance; they are penalty provisions for unauthorized electronic surveillance. However, if this reading were adopted, then the next question, discussed in 4 below, could be easier to answer.

Intermission.

Let's pause for a minute and review the bidding. The analysis so far is that (1) NSA was engaged in "electronic surveillance" as defined in FISA; (2) Congress in 1978 intended "electronic surveillance" to be conducted exclusively under FISA's procedures; and (3) those procedures permit electronic surveillance only as specifically authorized in FISA itself (although there is an alternative reading that FISA, through its civil and criminal penalty provisions, incorporates by reference any other statute that authorizes electronic surveillance). Those are relatively easy questions, but now I think it gets a little harder. The next question is whether Congress at some point after 1978 enacted legislation (or its equivalent) that changes the answer to the second question. In other words, did Congress implicitly repeal or amend the exclusivity provision set out in 18 U.S.C. § 2511(2)(f)? If not, the fifth and final question is the constitutional one – *Steel Seizure* on steroids – of whether Article II empowers the President to violate FISA.

4. Did Congress implicitly repeal or amend the exclusivity provision?

I haven't done a comprehensive review of legislation enacted after 1978, but the only law that has been cited as authority for the NSA program is the Authorization to use Military Force (AUMF),[4] enacted by Congress shortly after the September 11, 2001,

---

[4] Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001). The AUMF provides:

SECTION 1. SHORT TITLE.

This joint resolution may be cited as the "Authorization for Use of Military Force".

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) IN GENERAL—That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

(b) War Powers Resolution Requirements—

(1) SPECIFIC STATUTORY AUTHORIZATION—Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution.

(2) APPLICABILITY OF OTHER REQUIREMENTS—Nothing in this resolution supercedes any requirement of the War Powers Resolution.

terrorist attacks. In *Hamdi v. Rumsfeld*,[5] the Supreme Court held that the AUMF authorized the use of military detention. Although the AUMF did not refer specifically to such detention, it did authorize the President to use "all necessary and appropriate force" against "nations, organizations, or persons" associated with the September 11 attacks, and the Supreme Court held that in some situations, the detention "is so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use."[6]

It would not be difficult for the government to advance the same argument with respect to intelligence gathering, which has always been part of warfare. Although electronic surveillance is obviously of more recent vintage, even FISA's legislative history acknowledges that such surveillance has been conducted by all Presidents since technology allowed in the 19th and beginning of the 20th century. Electronic surveillance of telegraph signals was apparently conducted in the Civil War. See *Berger* v. *United States*, 388 U.S. 41, 45-46 (1967). Surveillance of purely domestic communications might raise separate issues than foreign or international surveillance,[7] but international communications between the U.S. and Afghanistan, or between the U.S. and other locations subject to the AUMF, seem at least arguably within the ambit of what the AUMF authorized.

The more difficult question is determining the effect of the AUMF in light of FISA's exclusivity provision. In *Hamdi*, Congress had enacted a statute, 18 U.S.C. § 4001(a), which provides that "[n]o citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress." The Supreme Court explained that "Congress passed § 4001(a) in 1971 as part of a bill to repeal the Emergency Detention Act of 1950, 50 U.S.C. § 811 et seq., which provided procedures for executive detention, during times of emergency, of individuals deemed likely to engage in espionage or sabotage. Congress was particularly concerned about the possibility that the Act could be used to reprise the Japanese internment camps of World War II."[8] The *Hamdi* Court found that the AUMF was an "Act of Congress" and that detention pursuant to it therefore satisfied Section 4001.

To read the AUMF to overcome FISA, the government probably would have to go one step further than the Court went in *Hamdi*. Where 18 U.S.C. § 4001 merely required an Act of Congress to authorize every detention, FISA's exclusivity provision provides that electronic surveillance may be conducted "exclusively" under FISA's procedures. To rely on the AUMF, therefore, the government would have to argue that it implicitly repealed the exclusivity provision. That is particularly the case because FISA

---

[5] 124 S. Ct. 2633 (2004).

[6] 124 S. Ct. at 2640

[7] *Compare Hamdi* (U.S. citizen first detained in Afghanistan), *with* Padilla v. Rumsfeld, 124 S. Ct. 2711 (2004) (U.S. citizen first arrested in the United States).

[8] 124 S. Ct. at 2639.

already contains an exception for surveillance and searches conducted for 15 days following a genuine declaration of war, 50 U.S.C. § 1811,[9] which the AUMF clearly was not. Congress has the authority to repeal the exclusivity provision, of course, but courts tend to disfavor implied repeals through ambiguous language.[10] On the other hand, reading the AUMF as an implied repeal would allow resolution of the case on statutory grounds, and thereby avoid a constitutional question, in keeping with the doctrine of constitutional avoidance.[11] My sense is that the AUMF was not – and would not be found by courts to be – an implied repeal of FISA's exclusivity provision, but I acknowledge that it's a hard question.

The result could be different if courts adopted the alternative reading of FISA discussed above. If FISA's "procedures" for electronic surveillance include those of any "statute," the case would be more like *Hamdi*, at least if a joint resolution passed by both Houses of Congress and signed by the President is a "statute" as that term is used in the civil and criminal penalty provisions of FISA.[12]

5. What happens if the NSA surveillance was prohibited by statute?

If courts conclude that the AUMF does not authorize the NSA surveillance – *e.g.*, because it does not repeal the exclusivity provision – then a constitutional issue likely arises. Does the President's Article II power allow him to authorize the NSA surveillance despite FISA? This is a monumental question, well beyond the scope of this little note. But I believe that the legal (and political) validity of the President's argument would turn in large part on the operational need for the surveillance and the need to eschew the use of FISA. To take a variant on the standard example, if the government had probable cause that a terrorist possessed a nuclear bomb somewhere in Georgetown, and was awaiting telephone instructions on how to arm it for detonation, and if FISA were interpreted not to allow surveillance of every telephone in Georgetown in those circumstances, the President's assertion of Article II power to do so would be quite persuasive. By contrast, claims that FISA simply requires too much paperwork or the bothersome marshaling of arguments seem relatively weak justifications for resorting to Article II power in violation of the statute. A lot turns on the facts.

-- David Kris
12-20-05

---

[9] "Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress."

[10] *See, e.g.*, United States v. Borden Co., 308 U.S. 188, 198 (1939).

[11] *Clark* v. *Martinez*, 543 U.S. 371, ___ (2005).

[12] Even if it does not repeal the exclusivity provision, the AUMF might add some patina of Congressional endorsement to the President's assertion of constitutional authority to violate FISA. Even if it did not shift the case out of Justice Jackson's third *Steel Seizure* category – where the President acts in contravention of Congress' will – it might represent at least a move on the "spectrum running from explicit congressional authorization to explicit congressional prohibition." *Dames & Moore* v. *Regan*, 453 U.S. 654, 669 (1981).