U. S. Department of Justice

Civil Division

Exhibit 3

Assistant Attorney General *Washington, D.C. 20530*

June 14, 2006

VIA FACSIMILE AND FEDERAL EXPRESS
The Honorable Zulima V. Farber
Attorney General of New Jersey
25 Market Street
Trenton, New Jersey 08625

Re: Subpoenas Duces Tecum Served on Telecommunications Carriers Seeking Information Relating to the Alleged Provision of Telephone Call History Data to the National Security Agency

Dear Attorney General Farber:

Please find attached the Complaint filed today by the United States in the United States District Court for the District of New Jersey, in connection with the subpoenas that you have served on various telecommunications companies (the "carriers") seeking information relating to those companies' alleged provision of "telephone call history data" to the National Security Agency ("NSA"). As set forth in the Complaint, it is our belief that compliance with the subpoenas would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security, and that enforcing compliance with these subpoenas would be inconsistent with, and preempted by, federal law.

The subpoenas infringe upon federal operations, are contrary to federal law, and accordingly are invalid under the Supremacy Clause of the United States Constitution for several reasons. The subpoenas seek to compel the disclosure of information regarding the Nation's foreign-intelligence gathering, but foreign-intelligence gathering is an exclusively federal function. Responding to the subpoenas, including disclosing whether or to what extent any responsive materials exist, would violate various specific provisions of federal statutes and Executive Orders. And the recent assertion of the state secrets privilege by the Director of National Intelligence in cases regarding the very same topics and types of information sought by your subpoenas underscores that any such information cannot be disclosed.

Although we have filed the attached Complaint at this juncture in light of the return date on the subpoenas (June 15), we nevertheless hope that this matter may be resolved amicably, and

that litigation will prove unnecessary. Toward that end, this letter outlines the basic reasons why, in our view, the state-law subpoenas are preempted by federal law. We sincerely hope that, in light of governing law and the national security concerns implicated by the subpoenas, you will withdraw them, thereby avoiding needless litigation. The United States very much appreciates your consideration of this matter.

1. There can be no question that the subpoenas interfere with and seek the disclosure of information regarding the Nation's foreign-intelligence gathering. But it has been clear since at least *McCulloch v. Maryland*, 4 U.S. 316 (1819), that state law may not regulate the Federal Government or obstruct federal operations. And foreign-intelligence gathering is an exclusively federal function; it concerns three overlapping areas that are peculiarly the province of the National Government: foreign relations and the conduct of the Nation's foreign affairs, *see American Insurance Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003); the conduct of military affairs, *see Sale v. Haitian Centers Council*, 509 U.S. 155, 188 (1993) (President has "unique responsibility" for the conduct of "foreign and military affairs"); and the national security function. As the Supreme Court of the United States has stressed, there is "paramount federal authority in safeguarding national security," *Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 76 n.16 (1964), as "[f]ew interests can be more compelling than a nation's need to ensure its own security." *Wayte v. United States*, 470 U.S. 598, 611 (1985).

The subpoenas demand that each carrier produce information regarding specified categories of communications between that carrier and the NSA since September 11, 2001, including "[a]ll names and complete addresses of Persons including, but not limited to, all affiliates, subsidiaries and entities, that provide Telephone Call History Data to the NSA";[1] any and all Executive Orders, court orders, or warrants "provided to [the carrier] concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll Documents concerning the basis for [the carrier's] provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; and "[a]ll Documents concerning any written or oral contracts, memoranda of understanding, memoranda of agreement, other agreements or correspondence by or on behalf of [the carrier] and the NSA concerning the provision of Telephone Call History Data to the NSA." See Document Requests, ¶¶ 1-13. In seeking to exert regulatory authority[2] with respect to the nation's foreign-intelligence gathering, you have thus sought to use your state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal

---

[1] "Telephone Call History Data" is defined as "any data [the carrier] provided to the NSA including, but not limited to, records of landline and cellular telephone calls placed, and/or received by [the carrier's] subscriber with a New Jersey billing address or New Jersey telephone number." Definitions, ¶8.

[2] The subpoenas make clear that they are "issued pursuant to the authority of N.J.S.A. 56:8-1 et seq., specifically N.J.S.A. 56:8-3 and 56:8-4."

prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 326-27, 4 L.Ed. 579 (1819) ("[T]he states have no power . . . to retard, impede, burden, or in any manner control, the operations of the constitutional laws enacted by Congress to carry into execution the power vested in the general government."); *see also Leslie Miller, Inc. v. Arkansas*, 352 U.S. 187 (1956).

The Supreme Court's decision in *American Insurance Ass'n v. Garamendi*, 539 U.S. 396 (2003), is the most recent precedent that demonstrates that these state-law subpoenas are preempted by federal law. In *Garamendi*, the Supreme Court held invalid subpoenas issued by the State of California to insurance carriers pursuant to a California statute that required those carriers to disclose all policies sold in Europe between 1920 and 1945, concluding that California's effort to impose such disclosure obligations interfered with the President's conduct of foreign affairs. Here, the subpoenas seek the disclosure of information that infringes on the Federal Government's intelligence gathering authority and on the Federal Government's role in protecting the national security at a time when we face terrorist threats to the United States homeland; those subpoenas, just like the subpoenas at issue in *Garmendi*, are preempted. Under the Supremacy Clause, "a state may not interfere with federal action taken pursuant to the exclusive power granted under the United States Constitution or under congressional legislation occupying the field." *Abraham v. Hodges*, 255 F.Supp. 2d 539, 549 (D.S.C. 2002) (enjoining the state of South Carolina from interfering with the shipment of nuclear waste, a matter involving the national security, because "when the federal government acts within its own sphere or pursuant to the authority of Congress in a given field, a state may not interfere by means of conflicting attempt to promote its own local interests").

2. Responding to the subpoenas, including merely disclosing whether or to what extent any responsive materials exist, would violate various federal statutes and Executive Orders. Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence ("DNI") the authority and responsibility to "protect intelligence sources and methods from unauthorized disclosure." *Ibid.*[3] (As set forth below, the DNI has determined that disclosure of the types of information sought by the subpoenas would harm national security.) Similarly, Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides: "[N]othing in this Act or

---

[3] The authority to protect intelligence sources and methods from disclosure is rooted in the "practical necessities of modern intelligence gathering," *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has been described by the Supreme Court as both "sweeping," *CIA* v. *Sims*, 471 U.S. 159, 169 (1985), and "wideranging." *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is the responsibility of the [intelligence community] to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency." *Ibid.*[4]

Several Executive Orders promulgated pursuant to the foregoing constitutional and statutory authority govern access to and handling of national security information. Of particular importance here, Executive Order No. 12958, 60 Fed. Reg. 19825 (April 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (March 25, 2003), prescribes a comprehensive system for classifying, safeguarding and declassifying national security information. It provides that a person may have access to classified information only where "a favorable determination of eligibility for access has been made by an agency head or the agency head's designee"; "the person has signed an approved nondisclosure agreement"; and "the person has a need-to-know the information." That Executive Order further states that "Classified information shall remain under the control of the originating agency or its successor in function." Exec. Order No. 13292, Sec. 4.1(c). Exec. Order No. 13292, Sec. 4.1(a).

It also is a federal crime to divulge to an unauthorized person specified categories of classified information, including information "concerning the communication intelligence activities of the United States." 18 U.S.C. § 798(a). The term "classified information" means "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution," while an "unauthorized person" is "any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States." 18 U.S.C. § 798(b).

New Jersey state officials have not been authorized to receive classified information concerning the foreign-intelligence activities of the United States in accordance with the terms of the foregoing statutes or Executive Orders (or any other lawful authority). To the extent your subpoenas seek to compel disclosure of such information to state officials, responding to them would obviously violate federal law.

---

[4] Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *The Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1389 (D.C. Cir. 1979). Thus, in enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures,'" *Hayden*, 608 F.2d at 1390 (citing legislative history), and "[t]he protection afforded by section 6 is, by its very terms, absolute. If a document is covered by section 6, NSA is entitled to withhold it. . . ." *Linder v. Nat'l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

3. The recent assertion of the state secrets privilege by the Director of National Intelligence ("DNI") in cases regarding the very same topics and types of information sought by your subpoenas underscores that compliance with those subpoenas would be improper. It is well-established that intelligence information relating to the national security of the United States is subject to the Federal Government's state secrets privilege. *See United States v. Reynolds*, 345 U.S. 1 (1953). The privilege encompasses a range of matters, including information the disclosure of which would result in an "impairment of the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign Governments." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), *cert. denied sub nom. Russo v. Mitchell*, 465 U.S. 1038 (1984) (footnotes omitted); *see also Halkin v. Helms*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects intelligence sources and methods involved in NSA surveillance).

In ongoing litigation in the United States District Court for the Northern District of California, the DNI has formally asserted the state secrets privilege regarding the very same topics and types of information sought by your subpoenas. *See Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.). In particular, the DNI's assertion of the privilege encompasses "allegations about NSA's purported involvement with AT&T," Negroponte Decl. ¶12, because "[t]he United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets." *Id.* ¶ 12. As DNI Negroponte has explained, "[t]he only recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor deny these sorts of allegations, regardless of whether they are true or false. To say otherwise when challenged in litigation would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general." Negroponte Decl. ¶12; *see also* Alexander Decl. ¶8. As DNI Negroponte has further explained, to disclose further details about the intelligence activities of the United States "would disclose classified intelligence information and reveal intelligence sources and methods, which would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States' national security interests." Negroponte Decl. ¶ 11. Those concerns are particularly acute when we are facing the threat of terrorist attacks on United States soil.

In seeking information bearing upon NSA's purported involvement with various telecommunications carriers, your subpoenas thus seek the disclosure of matters with respect to which the DNI already has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods. Accordingly, the state law upon which the subpoenas are based is inconsistent with and preempted by federal law as regards intelligence gathering, and also conflicts with the assertion of the state secrets privilege by the Director of National Intelligence. Any application of state law that would compel such disclosures notwithstanding the DNI's assessment would contravene

the DNI's authority and the Act of Congress conferring that authority. More broadly, the subpoenas involve an improper effort to use state law to regulate or oversee federal functions, and implicate federal immunity under the Supremacy Clause.

* * *

For the reasons outlined above, the United States believes that the subpoenas and the application of state law they embody are plainly inconsistent with and preempted under the Supremacy Clause, and that compliance with the subpoenas would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing harm to the national security. In this light, we sincerely hope that you will withdraw the subpoenas, so that litigation over this matter may be avoided.

Please do not hesitate to contact me if you have any questions. As noted, your consideration of this matter is very much appreciated.

Sincerely,

Peter D. Keisler

cc: Bradford A. Berenson, Esq.
John G. Kester, Esq.
John A. Rogovin, Esq.
Christine A. Varney, Esq.

Attachments