Gregory L. Castle
Senior Counsel
Legal Department

SBC Services, Inc.
525 Market Street
Room 2022
San Francisco, California 94105

415.778.1487 Phone
415.974.1999 Fax
gregory.castle@att.com

SENT VIA EMAIL AND OVERNIGHT DELIVERY

June 30, 2006

Carole J. Washburn
Executive Secretary, Washington Utilities
and Transportation Commission
1300 S. Evergreen Park Drive SW
P.O. Box 47250
Olympia, WA 98504-7250

Re: ACLU Request for Investigation, Docket Number UT-060856

AT&T Communications of the Pacific Northwest, Inc. ("AT&T") appreciates the opportunity to provide the Commission with this response to the Commission's Notice of Opportunity to Comment issued on June 2, 2006 in the above-referenced matter.

In response to the American Civil Liberties Union of Washington Foundation's ("ACLU") May 25, 2006 letter requesting the Commission to open an investigation, AT&T previously submitted a letter on May 26, 2006, which is incorporated by reference herein. In that letter, AT&T explained that the Commission could not investigate these issues because, under the controlling provisions of federal law, AT&T and other carriers are legally barred from providing the Commission with the information that would be required to conduct any such investigation. Since that letter was submitted, there have been significant developments in other related matters which starkly confirm any attempt by this Commission to investigate these matters would be unwise as a matter of policy and unsupportable as a matter of law.

Foremost, these points are dramatically underscored by what transpired in New Jersey when it attempted to investigate these issues. In particular, in mid-May of this year, the New Jersey Attorney General issued subpoenas seeking information regarding the activities of AT&T, Verizon, Qwest, and other carriers in connection with the alleged NSA Program. The return date for the subpoena was June 15, 2006. On June 14, United States filed an action in federal district court against the New Jersey Attorney General, AT&T Corp., Verizon, Qwest, and other carriers, seeking, among other things, a declaratory judgment that federal law prohibits New Jersey from enforcing the subpoenas and prohibits AT&T Corp. from providing the requested information to state officials ("New Jersey Action").[1] In its complaint, the United States contended that state

[1] *See* Complaint, United States of America v. Zulima V. Farber, et al., Civil Action No. 3:06 cv 02683, Prayer for Relief ¶ 1, (D.N.J.) (June 14, 2006) (Exh. A).

attempts to force carriers to disclose information about their activities, if any, under the NSA Program relate to exclusively federal functions and are preempted by a number of different provisions of federal law, including a number of statutes that bar the disclosure of classified national security information to state officials.

The United States explained the basis for these contentions in greater detail in a letter that was simultaneously sent to the New Jersey Attorney General.[2] There, the United States stated that state subpoenas seeking information relating to the NSA Program "intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives" and that "[r]esponding to the subpoenas," and even merely "disclosing whether or to what extent any responsive materials exist, would violate various specific provisions of federal statutes and Executive Orders," including provisions that carry criminal sanctions.[3] The United States also explained that the subpoenas "seek the disclosure of matters with respect to which the D[irector of] N[ational] I[intelligence] already has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods" in contravention of the United States' state secrets privilege.[4] In connection with this same lawsuit, the United States also sent a letter to AT&T Corp. that specifically warned AT&T Corp. that "[r]esponding to the subpoenas - including by disclosing whether or to what extent any responsive materials exist - would violate federal laws and Executive Orders."[5]

After this lawsuit was filed, AT&T Corp. has advised the New Jersey Attorney General that it cannot disclose any of the requested information regarding its activities, if any, under the NSA program, pending the final resolution of these issues in the federal judicial system. The New Jersey Attorney General then advised AT&T Corp. and the other carrier defendants that she would make no attempt to enforce the subpoena for at least the next 30 days, so there was no need for the United States to seek a TRO or a preliminary injunction to bar the New Jersey Attorney General from enforcing the subpoena or to bar the carriers from responding to it.

The experience in New Jersey demonstrates that any attempt by this Commission to investigate the role of carriers under the NSA program would have no effect other than to lead to another federal-state confrontation, which carriers would be required to respond to by refusing to provide any relevant information to this Commission. In light of the unequivocal actions and directions from the United States, AT&T will be no more able to respond to this Commission than it could respond to the subpoena of the New Jersey Attorney General.

In addition, events in New Jersey are not the only relevant developments that have occurred in the period since AT&T's Letter of May 26. In the first of the federal court lawsuits (*Hepting),* the district court issued an order on June 6 in which it agreed with United States and AT&T that there can be no discovery in this case unless and until the court conducts an *ex parte* and *in camera* review of the classified memorandum and classified depositions of Ambassador Negroponte and General Alexander and determines if the United States has properly invoked its

---

[2] *See* Letter from Peter D. Keisler to the Honorable Zulima V. Farber, (June 14, 2006) (Exh. B).
[3] *Id.* at 2-3.
[4] *Id.* at 5.
[5] *See* Letter from Peter D. Keisler to Bradford A. Berenson, Esq., et al., at 1 (June 14, 2006) (Exh. C).

military and state secrets privilege. The Court concluded that there is potential for "exceptionally grave damage to the national security of the United States" if information that would confirm or deny AT&T's participation in the program is publicly disclosed now.[6] Oral argument was heard on June 23, 2006 on the United States' motion to dismiss the *Hepting* case under the states secrets privilege.

In addition, there now are a total of 34 pending federal court class actions lawsuits claiming that carriers unlawfully disclosed calling records and other information to NSA, and the United States has made clear that it will assert the state secrets privilege in all these cases. In particular, in joining Verizon's motion to consolidate these cases in a single MDL court, the United States stated that "The United States Intends to Assert the State Secrets Privilege in All of the Pending Actions Brought and Seek their Dismissal."[7]

Further, during this period, other state utility commissions have decided not to investigate these issues. The Iowa commission entered an order that so provided on May 25, 2006.[8] Similarly, on June 20, 2006, the Delaware Commission announced that it will defer proceedings on the ACLU complaint that was filed before it for a period of at least six months, which is a period of time that this commission thought would be sufficient to allow the New Jersey action and the 34 pending private actions to progress to or near an initial resolution.[9]

In light of these developments, as well as those set forth in AT&T's letter dated May 26, 2006, set forth below are AT&T's answers to the Commission's questions.

1. Does WAC 480-120-202 or any other state law or regulation prohibit a regulated telephone company or its affiliated interests from providing customer telephone calling information to the National Security Agency (NSA)?

No. WAC 480-120-202 expressly adopts the Federal Communications Commission's rules (47 C.F.R. §§ 64.2003 through 64.2009) with regard to the privacy of customer proprietary network information. *See* WAC 480-120-202. These rules were promulgated "to implement Section 222 of the Communications Act of 1934, as amended, 47 U.S.C. § 222." 47 C.F.R. § 64.2001(b). Section 222 expressly provides that this information may be disclosed "as required by law." *See* 47 U.S.C. § 222(c)(1).

As set forth in response to questions 2, 3 and 4, this issue is governed exclusively by federal law. Thus WAC 480-120-202 or any other state law or regulation can in no way impair or impede or otherwise regulate the circumstances under which telecommunications carriers may cooperate with intelligence or national security activities conducted by the federal government.

---

[6] *See* June 6 Order, Hepting, et al. v. AT&T Corp., et al., Case No. C 06-0672-VRW, N.D.Ca (June 6, 2006) (Exh. D).

[7] *See* The United States' Motion for Transfer and Coordination Pursuant to 28 U.S.C. 1407 To Add Actions To MDL 1791 And Response to Verizon's Motion For Transfer and Coordination, at 12, In re National Security Agency Litigation, Judicial Panel on Multidistrict Litigation (June 19, 2006) (Exh. E).

[8] *See* Letter from David Lynch, General Counsel, Iowa Utilities Board to Mr. Frank Burdette (May 25, 2006) (Exh. F).

[9] The Delaware commission announced its decision in a public proceeding, the transcript of which is attached as Exh. G. A separate order will be issued hereafter.

2. Does the Commission have the legal authority to compel a regulated telephone company or its affiliates to disclose whether it had provided customer calling information to the NSA?

No. Controlling federal law prohibits the disclosure of this information. Foreign intelligence, foreign affairs, military, and national security matters are exclusively the province of the federal government, and any state law, regulation, or state governmental activity that would have a tendency to conflict, impair, impede, defeat, or affect such federal activities is wholly preempted under the Supremacy Clause of the United States Constitution.

The United States Constitution provides that federal law "shall be the supreme Law of the Land. . . ." Art. VI, cl. 2. Accordingly, it as long been settled "that state law that conflicts with federal law is 'without effect.'" *Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 516 (1992) (citations omitted). State law is preempted when federal law so thoroughly occupies a field that there is no room left for the states to regulate, or when there is a conflict between federal and state law, such as when federal law prohibits what state law purports to require. *See id.; see also Crosby v. Nat'l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (citations omitted) ("state law is preempted to the extent that it conflicts with federal law"). This is true whether the state law conflicts with federal statutory law or federal common law. *See, e.g., Boyle v. United Technologies Corp.*, 487 U.S. 500, 504 (1998) (there are some fields of activity that involve "'uniquely federal interests,' [and] are so committed by the Constitution and laws of the United States to federal control that state law is pre-empted and replaced, where necessary, by federal law of a content prescribed (absent explicit statutory directive) by the courts – so-called 'federal common law.'")(citations omitted). Thus where there are "uniquely federal interests," state law is preempted to the extent that there is a conflict between the two. *See id.* at 504-05, 507-08. Moreover, when unique federal interests are involved, "[t]he conflict with federal policy need not be as sharp as that which must exist for ordinary pre-emption when Congress legislates in a field which the States have traditionally occupied." *Id.* at 507. In light of these principles, there has never been any doubt that "the 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." *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 326-27 (1819).

AT&T cannot disclose whether any customer calling information has been provided to the NSA without direct conflict with at least two federal statutes, either one of which would be sufficient to preempt proceedings on this request. *See English v. Gen. Elec. Co.*, 496 U.S. 72, 79 (1990) (noting that "the Court has found pre-emption where it is impossible for a private party to comply with both state and federal requirements"). This position was clearly stated by the United States in its June 14, 2006 letter to New Jersey Attorney General in connection with the New Jersey Action. In that letter, the United States asserted that "[r]esponding to the subpoenas" issued by New Jersey, which sought national security information of the precise type that this Commission would necessarily have to seek if it proceeded in this matter, "including merely disclosing whether or to what extent any responsive material exists, would violate federal laws and Executive Orders."[10] In addition to the two statutes discussed below, the June 14 letter of

[10] *See* Exh. B at 3.

the United States details other binding provisions of federal law with which any state investigation of NSA intelligence activities would conflict.

First, 18 U.S.C. § 798 makes it a *felony* to "knowingly and willfully communicate[], furnish[], transmit[], or otherwise make[] available to an unauthorized person, or publish[], or use[] in any manner prejudicial to the safety or interest of the United States, . . . any classified information . . . concerning the communication intelligence activities of the United States." *Id.* The United States has repeatedly emphasized that the NSA program and all of its operational details, including the existence or non-existence of participation by particular telecommunication carriers, is highly classified. In his declaration filed in *Hepting*, Director Negroponte has sworn that "[t]o discuss [the Terrorist Surveillance Program] in any greater detail . . . would disclose classified information."[11]

Similarly, when Attorney General Gonzales made a limited public acknowledgement of an NSA program concerning "intercepts of contents of communications" involving al-Qaeda, he stressed that the program is not only "highly classified," but indeed "probably the most classified program that exists in the United States government."[12] Moreover, because the United States has asserted that the *Hepting* action should be dismissed because state secrets are at the core of the case, it can be presumed that allowing state actions pertaining to the NSA program to proceed could result in the disclosure of classified materials. *See Halkin v. Helms ("Halkin II")*, 690 F.2d 977, 996 n.69 (D.C. Cir. 1982) (noting that "matter qualifying as a secret of state will presumably always qualify for classified status."). Because AT&T cannot disclose any information, including the existence or non-existence of its cooperation in the NSA program, AT&T could not answer the complaint without violating this criminal statute.

Second, this request is also preempted by § 6 of the National Security Agency Act of 1959, Pub. L. No. 83-36, § 6, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note), which prohibits the disclosure of any information regarding the activities of the NSA. Specifically, the Act provides that "*nothing in this Act or 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." 50 U.S.C § 402 note (emphasis added).

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 1381, 1390 (D.C. Cir. 1979). This statute "reflects … a congressional judgment that, in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *Founding Church of Scientology v. National Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden*, 608 F.2d at 1389 (interpreting section 6; "release of the documents would disclose a function of the NSA, since signals intelligence is one of the Agency's primary functions; and would disclose information with respect to Agency activities, since any

---

[11] Negroponte Decl. ¶ 11; see also id. ¶ 13 ("proceedings in this case risk disclosure of privileged and classified intelligence-related information") (Exh. H); Alexander Decl. ¶ 9 (same) (Exh. I).

[12] *See* Press Conference of Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), available at http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

information about an intercepted communication concerns an NSA activity"); Thus, "[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).

Requiring disclosure of this information would clearly be in conflict with the Act. The Federal Communications Commission has already recognized that because "[t]he Commission has no power to order the production of classified information," and because section 6 of the National Security Act of 1959 independently prohibits disclosure of information relating to NSA activities, it lacked authority to compel the production of the information necessary to undertake an investigation and therefore declined to do so.[13] This Commission should reach the same conclusion here.

In addition to the specific conflicts described above, the very subject matter of the ACLU's request– AT&T's alleged cooperation with the federal government in its efforts to protect national security – is preempted entirely by federal law. Matters concerning national security are clearly and exclusively committed to the Executive Branch of the United States government. See U.S. Const. art. II, § 2, cl.1. ("The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual service of the United States. . . ."). The Supreme Court has repeatedly emphasized that matters involving national security and foreign affairs are within the exclusive province of the federal government, and in particular, the Executive Branch. *See Dep't of the Navy v. Egan,* 484 U.S. 518, 529 (1988); *Haig v. Agee*, 453 U.S. 280, 292 (1981); *Banco Nacional de Cuba v. Sabbatino*, 376 U.S. 398, 425 (1964); *United States v. Pink,* 315 U.S. 203, 233-34 (1942).

It is likewise clear that the gathering of foreign intelligence and the protection of the NSA program are vital components of the powers of the national executive. *See Haig*, 435 U.S. at 307 ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation. Protection of the foreign policy of the United States is a governmental interest of great importance, since foreign policy and national security concerns cannot be neatly compartmentalized. Measures to protect the secrecy of our Government's foreign intelligence operations plainly serve these interests.") (internal quotation marks and citations omitted). Moreover, the Supreme Court has recognized that only the Executive Branch is equipped to determine what information must be designated as classified and protected for national security reasons. *See Egan*, 484 U.S. at 529 (1988).

The ACLU's request is related to the intelligence gathering activities of the federal national security establishment that are designed to prevent further attacks on American soil as part of the nation's post-9/11 war effort. These activities are entirely the responsibility of the federal government and are controlled entirely by federal law, and therefore this claim is preempted. *See, e.g., Mite Corp. v. Dixon*, 633 F.2d 486, 491 (7th Cir. 1980) ("In the realms of national security and foreign affairs, state legislation has been impliedly preempted because both areas are of unquestionably vital significance to the nation as a whole."); *Stehney v. Perry*, 907 F. Supp. 806, 824 (D.N.J. 1995) ("State regulation in the area of national security is expressly

[13] Letter from Kevin J. Martin, Chairman Federal Communications Commission to the Honorable Edward J. Markey, at 1 (May 22, 2006) (Exh. J).

preempted by Article I, § 8 and Article II, § 2 of the Constitution.") (citing *Pennsylvania v. Nelson*, 350 U.S. 497, 504-05 (1956)). As the United States made clear in its June 14, 2006 letter to the New Jersey Attorney General in connection with the New Jersey Action, by seeking to investigate matters pertaining to the NSA's intelligence gathering activities, a State "intrudes upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives."[14]

Moreover, the subject matter of this request is entirely preempted because Congress has comprehensively regulated the field of telecommunications carriers' assistance to the federal government in conducting law enforcement and surveillance activities. *See Hillsborough County v. Automated Med. Labs.*, 471 U.S. 707, 713 (1985) (federal law preempts an entire field of state law when "the scheme of federal regulation is sufficiently comprehensive to make reasonable the inference that Congress left no room for supplementary state regulation") (internal quotation marks and citation omitted).

Congress has legislated in detail concerning the obligations of telecommunications carriers to assist federal law enforcement and intelligence agencies with electronic surveillance and has thereby left no room for the states to regulate in this area. First, by enacting the Communications Assistance to Law Enforcement Act ("CALEA"), 47 U.S.C. § 1001 *et seq.*, Congress has fully provided for the technical capabilities that telecommunications carriers must possess so that they are in a position to assist state and federal governments in surveillance activities. Title 47 U.S.C. § 1002(a) provides that, with certain exceptions, "a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of," among other things, "expeditiously isolating and enabling the government . . . to intercept" wire and electronic communications of a particular subscriber and "expeditiously isolating and enabling the government . . . to access call-identifying information that is reasonably available to the carrier." This Section further provides that, in the absence of an order compelling a telecommunications carrier to assist in a particular surveillance, only the Attorney General of the United States may file suit against a carrier for failure to comply with CALEA's requirements. *See* 18 U.S.C. § 2522; H. Rep. 103-827, pt. 1, at 28 ("In order to avoid disparate enforcement actions throughout the country which could be burdensome for telecommunications carriers, this authority is vested in the Attorney General of the United States through the Department of Justice and the Offices of the various United States Attorneys.").

Federal law also comprehensively regulates when and under what circumstances telecommunications carriers must provide assistance to the federal government in conducting surveillance. *See, e.g.*, 18 U.S.C § 2511 et seq. (the Wiretap Act). Pursuant to the Wiretap Act, the federal government may obtain an order that requires a telecommunications carrier to assist in surveillance activities and if necessary, implement the necessary technical capabilities to provide such assistance. *See id.* The Wiretap Act also regulates the circumstances in which telecommunications carriers may intercept communications on behalf of the federal government and disclose those communications to government agents. *See id.* § 2511(2).

[14] Exh. B at 2-3.

The Stored Communications Act, 18 U.S.C. § 2701 *et seq.* similarly regulates in detail the circumstances in which telecommunications carriers may (and sometimes must) disclose to others, including government agents, stored communications such as e-mail on central servers, or customer calling records. *See id.* § 2702, 2703. Likewise, the Foreign Intelligence Surveillance Act (FISA) authorizes the federal government to obtain an order directing telecommunications carriers to assist in foreign intelligence surveillance activities and to preserve the secrecy of such surveillance activities. *See* 50 U.S.C. § 1804(a)(4)[15] ; 50 U.S.C. § 1805(c)(2).[16]

Finally, the fact that federal law preempts the entire field of telecommunications carriers' participation in surveillance activities is further demonstrated by the fact that all of these statutes contain mechanisms for public and private enforcement and a corresponding set of litigation immunities granted to telecommunications carriers. *See, e.g.*, 18 U.S.C. §§ 2511, 2520, 2707; 50 U.S.C. §§ 1805(i), 1809-1810.

This complex and comprehensive statutory scheme demonstrates that Congress has occupied the entire field with respect to the cooperation of telecommunications carriers with the federal government's intelligence-gathering and surveillance activities. Particularly given that such activities implicate responsibilities exclusively belonging to the federal government, there is no room for state regulatory authority to be employed in any manner that would alter or affect these federally-regulated and authorized activities. Indeed, in the realm of national security, even state laws that do not necessarily conflict with the purpose of a similar federal law are preempted. *See Commonwealth of Pennsylvania v. Nelson*, 350 U.S. 497, 478-79 (1956) ("The precise holding of the court, and all that is before us for review, is that the Smith Act of 1940. . .which prohibits the knowing advocacy of the overthrow of the Government of the United States by force and violence, supersedes the enforceability of the Pennsylvania Sedition Act which proscribes the same conduct."). In *Nelson*, the Court noted that once Congress determines that a particular area of law is a "matter of vital national concern, it is in no sense a local enforcement problem." *Id.* at 482.

Here, the intent of Congress is clear: it has regulated the capabilities telecommunications carriers must have in order to assist the federal government in surveillance activities; the circumstances under which the federal government can order carriers to provide surveillance assistance; the circumstances under which the information can be disclosed; and the liabilities

---

[15]"With respect to electronic surveillance authorized by this subsection [i.e., without a court order], the Attorney General may direct a specified communication common carrier to--(A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and (B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain. The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid." *Id.*

[16]"An order approving an electronic surveillance under this section shall direct--. . . (B) that, upon the request of the applicant, a specified communication or other common carrier . . . furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier . . . is providing that target of electronic surveillance; (C) that such carrier . . . maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and (D) that the applicant compensate, at the prevailing rate, such carrier . . . for furnishing such aid." *Id.*

and immunities of carriers for furnishing such assistance. There is thus no room for state law, including this action, to regulate or otherwise interfere with this exclusive federal function.

Accordingly, the Commission does not have the legal authority to compel AT&T to disclose whether it has provided customer calling information to the NSA.

3. Does the Commission have the legal authority to compel regulated telephone companies or their affiliates to release relevant information about such allegations?

No. As set forth in the response to Questions 2 and 4, the Commission's jurisdiction to investigate this issue is preempted by federal law which prohibits the disclosure of even the existence or non-existence of any relationship between AT&T and the federal government in connection with the NSA Program. We note that even the Federal Communications Commission has concluded that it lacks the authority to compel the production of this classified information and thus has declined to open an investigation into this matter.[17]

4. Would an assertion of the military and state secrets privilege by the United States Government preclude the Commission from taking action against a regulated telecommunications company?

Yes. The state secrets privilege is a constitutionally-based privilege belonging exclusively to the Executive branch of the federal government that protects any information whose disclosure would result in "impairment of the nation's defense capabilities" or "disclosure of intelligence-gathering methods or capabilities." *Ellsberg v. Mitchell,* 709 F.2d 51, 57 (D.C. Cir. 1983). The invocation of state secrets must be made formally through an affidavit by "the head of the department which has control over the matter, after actual personal consideration by the officer." *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953). When the entire subject matter of a controversy is a state secret, then the matter must be dismissed outright, and no balancing of competing considerations are allowed or sufficient to override the privilege. *See, e.g., Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). Moreover, the state secrets privilege cannot be waived by a private party such as AT&T. *See Reynolds*, 345 U.S. 1 at 7.

The states secrets assertion in *Hepting* covers all details of the NSA program at issue here, including the identities of any carriers who may or may not be participating in it and their roles and responsibilities, if any. This position was reiterated by the United States in its June 14, 2006 letter to the New Jersey Attorney General in connection with the New Jersey Action. In that letter, the United States asserted that "[i]n seeking information bearing upon NSA's purported involvement with various telecommunications carriers," New Jersey sought "the disclosure of matters with respect to which the DNI has already determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods."[18] The Justice Department then made clear that, as a legal matter, the state's effort to investigate matters covered by the privilege "conflicts with the assertion of the state secrets privilege by the Director of National Intelligence" and, as

[17] Letter from Kevin J. Martin, Chairman Federal Communications Commission to the Honorable Edward J. Markey, at 1 (May 22, 2006) (Exh. J).
[18] *See* Exh. B at 5.

such, "would contravene the DNI's authority and the Act of Congress conferring that authority."[19]

Because the United States has asserted the states secrets privilege with regard to even the mere existence or non-existence of any relationship between the federal government and AT&T in connection with this program, this state action is clearly in conflict with a controlling principle of federal law and cannot go forward.

In addition to the state secrets privilege, the ACLU's request must also be denied because well established federal law prohibits any adjudication of claims (state or federal) that relate to the existence of alleged espionage relationships with the United States. The so-called *Totten* bar provides that "the existence of a contract for secret services with the government is itself a fact not to be disclosed." *Totten v. United States*, 92 U.S. 105, 107 (1875). Just last year, the Supreme Court unanimously reaffirmed the *Totten* bar, holding that "lawsuits premised on alleged espionage agreements are altogether forbidden." *Tenet v. Doe*, 544 U.S. 1, 9 (2005). The Court described the "core concern" of *Totten* as "preventing the existence of [the alleged espionage agent's] relationship with the Government from being revealed." *Id.* at 10. Where this concern is present, an "absolute protection" is required, because "[t]he possibility that a suit may proceed and an espionage relationship may be revealed ... is unacceptable." *Id.* Indeed, the Supreme Court has observed that the applicability of the *Totten* bar may be decided before jurisdictional questions are resolved, and when the existence of a secret espionage agreement is at issue, the suit should be dismissed on the pleadings. *See Tenet*, 544 U.S. at 6 (describing the applicability of the Totten rule as a "'threshold question'"); *see id.* at 9 (noting that cases such as Totten in which "'the very subject matter of the action, a contract to perform espionage, was a matter of state secret" should be "'dismissed on the pleadings without ever reaching the question of evidence, since it [is] so obvious that the action should never prevail over the privilege'") (quoting *United States v. Reynolds,* 345 U.S. 1, 11 n.26 (1953) (emphasis in *Tenet*).

The concerns that are addressed by the *Totten* bar are squarely implicated by the ACLU's request. The request presents precisely the sort of claim that cannot be examined or adjudicated without attempting to establish the existence or non-existence of a secret espionage relationship between the United States and private parties. Accordingly, this federal rule of law preempts state law under these circumstances and, for this reason as well, this proceeding cannot proceed.

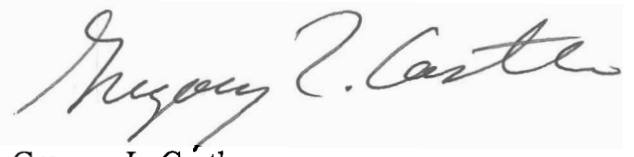
5. If the Commission decides to investigate the matter raised in the ACLU's May 25, 2006, letter, which procedural options would be most appropriate? (e.g., informal investigation, formal investigation, complaint).

Because controlling federal law prohibits the disclosure of any information called for in the request by the ACLU, including even the existence or non-existence of any relationship between AT&T and the federal government in connection with the NSA Program, this request cannot proceed under any procedure. Any investigation would likely merely result in the same sort of litigation already ongoing in the New Jersey Action.

---

[19] *Id.* at 2-3.

Sincerely,



Gregory L. Castle
Senior Counsel

cc: Dan Foley, General Attorney & Assistant General Counsel, AT&T Services, Inc.
David W. Carpenter, Sidley Austin LLP