



DIVISION OF
CORPORATION FINANCE

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549-3010

DC

February 9, 2007

Wayne A. Wirtz
Assistant General Counsel
Legal Department
AT&T Inc.
175 E. Houston, Room 205
San Antonio, TX 78205

Act: 1934
Section: _____
Title: HA-8
Public: _____
Availability: 2/9/2007

Re: AT&T Inc.
Incoming letter dated December 11, 2006

Dear Mr. Wirtz:

This is in response to your letters dated December 11, 2006 and January 19, 2007 concerning the shareholder proposal submitted to AT&T by Jeremy Kagan and co-proponents Jeffrey Hersh, Calvert Asset Management Company, Inc., Larry Fahn, the Adrian Dominican Sisters, and the Camilla Madden Charitable Trust. We also have received letters on behalf of the proponents dated January 9, 2007 and February 5, 2007. Our response is attached to the enclosed photocopy of your correspondence. By doing this, we avoid having to recite or summarize the facts set forth in the correspondence. Copies of all of the correspondence also will be provided to the proponents.

In connection with this matter, your attention is directed to the enclosure, which sets forth a brief discussion of the Division's informal procedures regarding shareholder proposals.

PROCESSED

MAR 02 2007

THOMSON
FINANCIAL

Sincerely,

David Lynn
Chief Counsel

Enclosures

cc: Conrad B. MacKerron
Director, Corporate and Social Responsibility Program
As You Sow
311 California Street, Suite 510
San Francisco, CA 94104



07045839

DC

Larry Fahn
Executive Director
As You Sow
311 California Street, Suite 510
San Francisco, CA 94104

Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
Adrian Dominican Sisters
1257 East Siena Heights Drive
Adrian, MI 49221-1793

Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
Camilla Madden Charitable Trust
1257 East Siena Heights Drive
Adrian, MI 49221-1793



Wayne A. Wirtz
Assistant General Counsel
Legal Department
AT&T Inc.
175 E. Houston, Room 205
San Antonio, Texas 78205
Ph. (210) 351-3736
Fax (210) 351-3467

1934 Act/ Rule 14a-8

December 11, 2006

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, DC 20549

Re: AT&T Inc. 2007 Annual Meeting
Stockholder Proposal of Jeremy Kagan

RECEIVED
2006 DEC 12 PM 3:48
OFFICE OF CHIEF COUNSEL
DIVISION OF CORPORATION FINANCE

Ladies and Gentlemen:

This statement and the material enclosed herewith are submitted on behalf of AT&T Inc. ("AT&T") pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended. AT&T has received a stockholder proposal from "As You Sow," on behalf of Jeremy Kagan, for inclusion in AT&T's 2007 proxy materials. The proposal was co-filed by Jeffrey Hersh, Calvert Asset Management Company, Inc., Larry Fahn, The Adrian Dominican Sisters, and Camilla Madden Charitable Trust (collectively, together with Jeremy Kagan, referred to hereinafter as "Proponents"). Proponents Kagan, Hersh and Calvert have requested that all communications be directed to As You Sow. For the reasons stated below, AT&T intends to omit this proposal from its 2007 proxy statement. It is important to note that AT&T has neither confirmed nor denied the existence of any of the programs that are the basis of this proposal, nor does AT&T now confirm or deny that it has participated in any such activities or programs. In fact, as described in the attached opinion from Sidley Austin LLP, to the extent AT&T were to have participated in any such programs, implementation of the proposal would cause AT&T to violate federal statutes prohibiting their disclosure.

Pursuant to Rule 14a-8(j), enclosed are six copies of each of: this statement, the opinion of Sidley Austin LLP, and the Proponents' letter submitting the proposal, which is attached to the referenced opinion. A copy of this letter and related cover letter are being mailed concurrently to As You Sow and Proponents Fahn, Adrian Dominican

Sisters and Camilla Madden Charitable Trust advising them of AT&T's intention to omit the proposal from its proxy materials for the 2007 Annual Meeting.

The Proposal

On October 27, 2006, AT&T received a letter from As You Sow, on behalf of Proponent Kagan, alleging that AT&T provided certain customer information to the National Security Agency ("NSA"), the Federal Bureau of Investigation ("FBI"), and other government agencies. The letter also contains a proposal, subsequently co-filed by the other Proponents, requesting that AT&T report on the technical, legal and ethical policy matters and other details relating to the alleged actions (the "Proposal"). Specifically, the Proposal states:

RESOLVED: That shareholders request that the Board of Directors issue a report to shareholders in six months, at reasonable cost and excluding confidential and proprietary information, which describes the following:

- The overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigations, NSA and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies;
- Any additional policies, procedures or technologies AT&T could implement to further ensure (a) the integrity of customers' privacy rights and the confidentiality of customer information, and (b) that customer information is only released when required by law; and
- AT&T's past expenditures on attorney's fees, experts fees, operations, lobbying and public relations/media expenses, relating to this alleged program.¹

The Proposal May be Omitted from the Proxy Statement Pursuant to Rule 14a-8(i)(2): Implementation of the Proposal by AT&T would violate federal law.

Rule 14a-8(i)(2) provides that a shareholder proposal may be excluded if it "would, if implemented, cause the company to violate any state, federal, or foreign law to which it is subject." The underlying premise of the Proposal is that AT&T has provided certain customer information to the NSA and other government agencies and that any such action would constitute a violation of the law and the privacy rights of customers. The

¹ The full text of the Proposal and its Supporting Statement is attached as Exhibit 1 to the opinion of Sidley Austin LLP.

Proposal would require the company to publish a report on the technical, legal and ethical policy matters and other details relating to the alleged actions.

The Proposal, by its terms, directly addresses information regarding the alleged communications intelligence activities of the United States. Any such activities, if engaged in by AT&T, would be classified and disclosing them would be prohibited under Federal law.

AT&T has obtained a legal opinion from the law firm of Sidley Austin LLP which describes in detail the laws governing the disclosure of the alleged activities involving the NSA, FBI and other government agencies (the "Sidley Austin Opinion").² The Sidley Austin Opinion confirms that the actions called for by the Proposal, based on the premise of the Proposal, would cause AT&T to violate a series of Federal laws designed to protect the intelligence gathering activities of the United States, including 18 U.S.C. § 798(a), which specifically prohibits knowingly and willfully divulging to an unauthorized person classified information regarding the communications intelligence activities of the United States.

Because these issues are discussed at considerable length in the Sidley Austin Opinion, that discussion is incorporated in this letter and will not be repeated here.

Since implementation of the Proposal would violate federal law, AT&T can exclude the Proposal from its 2007 proxy materials in accordance with Rule 14a-8(i)(2).

The Proposal May be Omitted from the Proxy Statement Pursuant to Rule 14a-8(i)(7): The Proposal relates to ordinary business matters.

Rule 14a-8(i)(7) permits a company to omit a shareholder proposal from its proxy materials if the proposal deals with a matter relating to the company's ordinary business operations. The general policy underlying the "ordinary business" exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting." This general policy reflects two central considerations: (i) "certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight"; and (ii) the "degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Exchange Act Release No. 34-40018 (May 21, 1998).

In applying the Rule 14a-8(i)(7) exclusion to proposals requesting companies to prepare reports on specific aspects of their business, the Staff has determined that it will consider whether the subject matter of the special report involves a matter of ordinary business. If it does, the proposal can be excluded even if it requests only the

² The Sidley Austin Opinion is attached to this letter as Attachment A.

preparation of the report and not the taking of any action with respect to such ordinary business matter. Exchange Act Release No. 34-20091 (August 16, 1983).³

The Proposal relates to ongoing litigation involving the company.

The Proposal may be omitted as a matter involving ordinary business because it would improperly interfere with AT&T's legal strategy and the discovery process in at least 20 pending proceedings that to Proponent Kagan allege unlawful acts by AT&T in relation to alleged provision of information to the NSA.

AT&T is presently the defendant in multiple pending lawsuits and other proceedings that generally allege that the company has violated customer privacy rights by providing information and assistance to government entities without proper legal authority, including allegedly providing information to the specific entities described in the proposal. For example, in *Terkel & American Civil Liberties Union of Illinois v. AT&T*, No. 06 C 2837 (N.D. Ill.), plaintiffs alleged that AT&T has provided the National Security Agency with access to calling records of millions of customers in the absence of a court order, warrant, subpoena, or certification from the Attorney General that no such process was required. Similarly, these same allegations were also made in *Hepting v. AT&T*, No. 3:06-CV-006720-VRW (N.D. Cal.), where the plaintiffs also alleged that AT&T had also acted unlawfully by providing the National Security Agency with the contents of communications in the absence of a court order, warrant, or certification from the Attorney General that no such process was required. There are over 20 pending cases that make one or both of these allegations, and these cases have been consolidated for coordinated pretrial proceedings in the United States District Court for the Northern District of California.

In addition, local chapters of the ACLU⁴ have filed complaints with over 20 state utility commissions that allege that AT&T violated state or federal law by providing the NSA with access to customer calling records in the absence of proper legal process. In cases where a state commission has attempted to institute an investigation, the United States has filed actions against AT&T and the state commissions, seeking declarations that these investigations are preempted by federal law and other appropriate relief.⁵

³ This Release addressed Rule 14a-8(c)(7), which is the predecessor to Rule 14a-8(i)(7).

⁴ We note that the web site of the American Civil Liberties Union claims responsibility for "The ACLU Freedom Files," a film, co-executive produced and directed by Proponent Kagan, and that, according to the ACLU web site, alleges that the civil liberties of America are threatened and describes how they have fought back. In the "Viewers Guide," the ACLU repeats the allegation that "Americans' phone calls and e-mails [are monitored] – without court approval. Proponent Kagan now seeks the same information through the shareholder approval process that the ACLU has sought through litigation.

⁵ See *United States v. Zulima V. Farber, et al.*, Civil Action No. 3:06 cv 02683 (D.N.J.); *United States v. Palermino, et al.*, C.A. 3:06-1405 (D. Conn.); *United States v. Adams, et al.*, C.A. 1:06-97 (D. Me.); *United States v. Gaw, et al.*, C.A. 4:06-1132 (E.D. Mo); *United States v. Volz, et al.*, C.A. 2:06-00188 (D. Vt.).

The Proposal repeats the substance of the complaints by repeating the allegation that AT&T "has voluntarily provided customer phone records and communications data to the National Security Agency." The Proposal goes on to call for a report on the policies "surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA and other government agencies without a warrant", disclosure of "AT&T's past expenditures on attorney's fees, experts fees, operations . . . relating to this alleged program, and a report on actions AT&T could take to "further" protect customer information, presumably from the government. All of these matters go directly to the substance of the complaints. The proposal calls for the same information that the plaintiff ACLU and others seek in discovery but sidesteps and interferes with the discovery process.

The Staff has previously acknowledged that a shareholder proposal is properly excludable under the "ordinary course of business" exception when the subject matter of the proposal is the same as or similar to that which is at the heart of litigation in which a registrant is then involved. See, e.g., Reynolds American Inc. (February 10, 2006) (proposal to notify African Americans of the purported health hazards unique to that community that were associated with smoking menthol cigarettes while the company was a defendant in a case alleging the company marketed menthol cigarettes to the African American community was excludable as ordinary business.); R. J. Reynolds Tobacco Holdings, Inc. (February 6, 2004) (proposal requiring company to stop using the terms "light," "ultralight" and "mild" until shareholders can be assured through independent research that such brands reduce the risk of smoking-related diseases excludable under the "ordinary course" exception because it interfered with litigation strategy of class-action lawsuit on similar matters); R. J. Reynolds Tobacco Holdings, Inc. (March 6, 2003) (proposal requiring the company to establish a committee of independent directors to determine the company's involvement in cigarette smuggling excludable under the "ordinary course" exception because it relates to subject matter of litigation in which the registrant was named as a defendant).

This result is also consistent with the longstanding position of the Staff that a registrant's decision to institute or defend itself against legal actions, and decisions on how it will conduct those legal actions, are matters relating to its ordinary business operations and within the exclusive prerogative of management. See, e.g., NetCurrents, Inc. (May 8, 2001) (proposal requiring NetCurrents, Inc. to bring an action against certain persons excludable as ordinary business operations because it relates to litigation strategy); Microsoft Corporation (September 15, 2000) (proposal asking the registrant to sue the federal government on behalf of shareholders excludable as ordinary business because it relates to the conduct of litigation); Exxon Mobil Corporation[*21] (March 21, 2000) (proposal requesting immediate payment of settlements associated with Exxon Valdez oil spill excludable because it relates to litigation strategy and related decisions); Philip Morris Companies Inc. (February 4, 1997) (proposal recommending that Philip Morris Companies Inc. voluntarily implement certain FDA regulations while simultaneously challenging the legality of those regulations excludable under clause (c)(7), the predecessor to the current (i)(7)); Exxon Corporation (December 20, 1995) (proposal

that registrant forego any appellate or other rights that it might have in connection with litigation arising from the Exxon Valdez incident excludable because litigation strategy and related decisions are matters relating to the conduct of the registrant's ordinary business operations).

Therefore, the Proposal directly implicates issues that are the subject matter of multiple lawsuits involving AT&T. In effect, the Proposal recommends that AT&T facilitate the discovery of the opposing parties in these various lawsuits at the same time the company is challenging those parties' legal positions or claims. Compliance with the Proposal would improperly interfere with AT&T's litigation strategy in these cases and intrude upon management's appropriate discretion to conduct the ordinary business litigation as its business judgment dictates.

The Proposal relates to matters of customer privacy.

The Staff has, in the past, applied Rule 14a-8(i)(7) to allow for the exclusion of proposals requesting reports on issues related to customer privacy. In Bank of America Corp., a shareholder, in response to specific instances of lost and stolen customer records, submitted a proposal requesting that the company prepare a report on its policies and procedures for ensuring the confidentiality of customer information. The Staff concluded that the requested report involved matters of ordinary business in that it sought information regarding the company's "procedures for protecting customer information" and concurred in the company's decision to exclude the proposal pursuant to Rule 14a-8(i)(7). Bank of America Corp. (February 21, 2006); see also, Bank of America Corp. (March 7, 2005) (an almost identical proposal from the same proponent was excluded as relating to the company's ordinary business of protecting customer information); Applied Digital Solutions, Inc. (March 25, 2006) (a proposal requesting the company to prepare a report analyzing the public privacy implications of its radio frequency identification chips was excluded as relating to the company's ordinary business of managing the privacy issues related to its product development).

Like the proposals excluded in Bank of America Corp., the Proposal requests AT&T to produce a report assessing customer privacy issues and the company's policies and procedures for addressing such issues, in response to a perceived breach of that privacy. Thus, the Proposal explicitly deals with matters of customer privacy, which are a central function of AT&T's daily business operations and cannot, "as a practical matter, be subject to direct shareholder oversight."

The Proposal relates to matters of legal compliance.

The Proposal can also be properly excluded, pursuant to Rule 14a-8(i)(7), because it seeks to regulate the company's conduct of its legal compliance program. The Staff has long since identified a company's compliance with laws and regulations as a matter of ordinary business. In Allstate Corp., a shareholder proposal requested, in part, that the company issue a report discussing the illegal activities that were the subject of a number of state investigations and consent decrees involving Allstate. The Staff held

that a company's general conduct of a legal compliance program was a matter of ordinary business and agreed to Allstate's exclusion of the proposal under Rule 14a-8(i)(7). Allstate Corp. (February 16, 1999); see also, Duke Power Co. (February 1, 1988) (a proposal requesting the company to prepare a report detailing its environmental protection and pollution control activities was excluded as relating to the ordinary business matter of complying with government regulations); Halliburton Company (March 10, 2006) (a proposal requesting the company to produce a report analyzing the potential impact on reputation and stock value of the violations and investigations discussed in the Proposal and discussing how the company intends to eliminate the reoccurrence of such violations was excluded as relating to the ordinary business of conducting a legal compliance program); Monsanto Co. (November 3, 2005) (a proposal requesting the company to issue a report on its compliance with all applicable federal, state and local laws was excluded as relating to the ordinary business of conducting a legal compliance program).

The essence of the Proposal is to discover the relationship, if any, between AT&T and government agencies, including those agencies responsible for matters of tax collection, fugitive apprehension, criminal prosecution, and national security, among others. Specifically, the Proposal looks for the technical, legal and policy issues related to the company's cooperation with the NSA, FBI and other government agencies, the effects that such cooperation may have on customers, and the costs associated with such cooperation. In addition, the proposal requests consideration of "additional policies, procedures or technologies that AT&T could implement to further ensure . . . (b) that customer information is only released when required by law." The information requested by the Proposal relates to AT&T's compliance with government laws and regulations and is precisely the type of information that the Staff has identified as relating to matters of ordinary business.

It would be hard to find matters that are more intimately related to day-to-day business operations, or that pose a greater threat to micro-manage the company, than a company's compliance with its legal obligations. Legal compliance is exactly the type of "matter of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment."

Moreover, AT&T believes that exclusion of the Proposal is justified because the Proposal involves the company in the political or legislative process relating to aspects of the company's operations. Numerous no-action precedents have indicated that proposals requesting a company to issue reports analyzing the potential impacts on the company of proposed national legislation may properly be excluded as "involving [the company] in the political or legislative process relating to an aspect of [the company's] operations." International Business Machines Corp. (March 2, 2000); see also, Electronic Data Systems Corp. (March 24, 2000) and Niagara Mohawk Holdings, Inc. (March 5, 2001) (in all three cases, proposals requesting the company to issue reports evaluating the impact on the company of pension-related proposals being considered by national policy makers were excluded as involving the company in the political or legislative process). Likewise, the Proposal essentially requests AT&T to evaluate the

impact that the alleged government surveillance programs would have on the company's business operations, including matters of customer privacy and company costs. In this way, the Proposal can be seen as involving AT&T in the political process, and, therefore, excludable as relating to the company's ordinary business.

The Proposal can be excluded as relating to matters of ordinary business, regardless of whether or not it touches upon a significant social policy issue.

Simply because a proposal touches upon a matter with possible public policy implications does not necessarily undermine the basis for omitting it under Rule 14a-8(i)(7). The Staff has indicated that the applicability of Rule 14a-8(i)(7) depends largely on whether implementing the proposal would have broad public policy impacts outside the company, or instead would deal only with matters of the company's internal business operations, planning and strategies. In fact, the Staff has consistently concurred with the exclusion of proposals that address ordinary business matters, even though they might also implicate public policy concerns. See, e.g. Microsoft (September 29, 2006) (excluding a proposal asking the company to evaluate the impact of expanded government regulation of the internet); Pfizer Inc. (January 24, 2006) and Marathon Oil (January 23, 2006) (excluding proposals requesting inward-looking reports on the economic effects of HIV/AIDS, tuberculosis and malaria pandemics on the companies' business strategies and risk profiles). The Proposal falls squarely in this group.

The Proposal requests that the company issue a report on matters relating to its ordinary business and, as such, may be properly omitted pursuant to Rule 14a-8(i)(7).

The Proposal May be Omitted from the Proxy Statement Pursuant to Rules 14a-8(i)(3) and 14a-8(i)(6): The Proposal is vague and indefinite and, therefore, AT&T would lack the power or authority to implement it.

Rule 14a-8(i)(3) permits a company to exclude a shareholder proposal if it is contrary to any of the Commission's proxy rules, including Rule 14a-9's prohibition on materially false and misleading statements in proxy solicitation materials.

The Proposal, by its own terms, is inherently contradictory - according to the Proposal, AT&T is, at the same time, required to provide information and permitted to exclude the same information. The underlying premise of the Proposal is that AT&T has participated in programs requiring it to provide customer information to the NSA and other government agencies, and the Proposal requests the company to provide information regarding such participation. Although, as noted above, AT&T has not confirmed or denied its participation in any such programs, the Proposal, itself, acknowledges that, if AT&T were a participant in these programs, information regarding its participation would be considered confidential. The Sidley Austin Opinion confirms that the essential portion of the information requested by the Proposal, if it existed, would be identified by the United States as classified information and must be treated

confidentially.⁶ However, the Proposal specifically allows AT&T to exclude all "confidential and proprietary information." These conflicting mandates make the Proposal inherently vague and indefinite and, as such, impossible for AT&T to implement. Therefore, the Proposal can be excluded under the Staff's interpretations of Rules 14a-8(i)(3) and 14a-8(i)(6).

Pursuant to the Staff's explanation of "materially false and misleading," a proposal can be properly excluded under Rule 14a-8(i)(3) where "the resolution contained in the proposal is so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (CF) (September 15, 2004); see also, Philadelphia Electric Co. (July 30, 1992). Moreover, the Staff has found a proposal to be sufficiently vague and indefinite so as to justify exclusion under Rule 14a-8(i)(3) where a company and its shareholders might interpret the proposal so differently that "any action ultimately taken by the company upon implementation of the proposal could be significantly different from the actions envisioned by the shareholders voting on the proposal." Fuqua Industries, Inc. (March 12, 1991).

Furthermore, Rule 14a-8(i)(6) allows for the exclusion of a shareholder proposal if the company lacks the power or authority to implement it. The Staff has previously held that a proposal may be omitted under Rule 14a-8(i)(6) where the proposal is so vague and indefinite that the company is unable to determine what actions are required by the proposal and, as such, is "beyond the [company's] power to effectuate." Int'l Business Machines Corporation (January 14, 1992) (permitted the exclusion of a resolution stating only that "It is now apparent that the need for representation has become a necessity."); see also, The Southern Company (February 23, 1995) (permitted the exclusion of a proposal recommending that the company take the essential steps to ensure the highest standards of ethical behavior of employees appointed to serve in the public sector without providing any suggestions on how to achieve such an objective).

Since substantially all of the information requested by the Proposal is confidential, the Proposal essentially requests AT&T to produce a report excluding the very substance of the report. Thus, the terms of the Proposal are so vague and ambiguous that it is impossible for AT&T to be able to ascertain with any reasonable certainty the exact actions that it would be required to take with respect to the Proposal. As such, the Proposal, if adopted, would be beyond AT&T's "power to effectuate." If AT&T were to implement the Proposal as drafted, it would issue a report excluding substantially all of the information sought for by the Proposal; this could result in a significantly different outcome than that envisioned by the shareholders voting on the Proposal.

⁶ For further analysis, refer to the Sidley Austin Opinion.

Because the terms of the Proposal are inherently vague and indefinite, AT&T believes that it can properly omit the Proposal from its proxy materials under Rules 14a-8(i)(3) and 14a-8(i)(6).

* * *

For the reasons set forth above, we ask the Staff to recommend to the Commission that no action be taken if the Proposal is omitted from AT&T's 2007 proxy statement. Please acknowledge receipt of this letter by date-stamping and returning the extra enclosed copy of this letter in the enclosed self-addressed envelope. If the Staff does not concur that AT&T may exclude the Proposal, we respectfully request that the decision be promptly appealed to the full Commission for reconsideration, and that we be promptly notified of that appeal.

Sincerely,



Wayne Wirtz
Assistant General Counsel

Enclosures

cc: As You Sow
Calvert Asset Management Co., Inc.
Larry Fahn
Camilla Madden Charitable Trust
Adrian Dominican Sisters



SIDLEY AUSTIN LLP
 1501 K STREET, N.W.
 WASHINGTON, D.C. 20005
 (202) 736 8000
 (202) 736 8711 FAX

bberenson@sidley.com
 (202) 736-8971

BEIJING	GENEVA	SAN FRANCISCO
BRUSSELS	HONG KONG	SHANGHAI
CHICAGO	LONDON	SINGAPORE
DALLAS	LOS ANGELES	TOKYO
FRANKFURT	NEW YORK	WASHINGTON, DC

FOUNDED 1888

November 22, 2006

Board of Directors
 AT&T Inc.
 c/o James D. Ellis
 General Counsel
 175 E. Houston, Room 205
 San Antonio, Texas 78205

Re: Shareholder Proposal

Ladies and Gentlemen:

You have requested our legal opinion whether implementation by AT&T Inc. ("AT&T" or the "Company") of a shareholder proposal submitted by Jeremy Kagan on October 24, 2006, along with several co-filers (the "Proposal") to the Company for inclusion in its 2007 proxy statement for AT&T Inc. ("Proxy") would violate federal law.¹

The Proposal. The Proposal calls for the AT&T Board of Directors to issue a report to shareholders describing, *inter alia*, "[t]he overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA [National Security Agency] and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies. . . ." The Proposal also would require the disclosure of past corporate expenditures, including for "operations" of specified intelligence programs allegedly undertaken by the NSA.

The cover letter accompanying the Proposal makes clear that it is based on the widely publicized allegations that AT&T and other telecommunications carriers have assisted the United States government, and in particular the NSA, in connection with foreign intelligence-gathering activities.² These media reports alleged two types of activities. First, on December 19, 2005, in response to a report in the *New York Times*, President Bush acknowledged the existence of a counterterrorism program involving the interception of international telephone calls made or

¹ The Proposal and cover letter are attached hereto as Exhibit 1.

² See Letter from Conrad B. MacKerron, Director, Corporate Social Responsibility Program to Edward E. Whitacre, CEO, AT&T Inc. (October 24, 2006) ("MacKerron Letter") (Exhibit 1) ("We are concerned about reports that AT&T provided customer information to the National Security Agency without a warrant.").

Board of Directors
AT&T Inc.
November 22, 2006
Page 2

received by suspected al Qaeda agents (the "Terrorist Surveillance Program").³ The United States Department of Justice subsequently published an explanation of the legal authority for the program acknowledged by the President and defended by the Attorney General.⁴ The United States has never publicly confirmed or denied the participation of any particular telecommunications carrier in the Terrorist Surveillance Program.

Subsequently, on May 11, 2006, *USA Today* published a story suggesting that the NSA's intelligence-gathering activities may also have included some form of access to domestic call records databases ("Calling Records Program").⁵ The United States has never publicly confirmed or denied either the existence of a Calling Records Program or the participation of any particular telecommunications carrier in a Calling Records Program. We shall refer to the Terrorist Surveillance Program and Calling Records Program together as the "Programs."

AT&T cannot confirm or deny any reports alleging participation in federal intelligence activities, including the Programs. For purposes of responding to your request only, we accept at face value the asserted facts reported in the newspapers and targeted by the Proposal. No inference can or should be drawn from these assumptions made only for purposes of this analysis regarding the truth or falsity or any such allegations, and nothing herein should be construed as an admission or denial of any allegation relating to such Programs.

Analysis. The United States has expressly and formally advised AT&T on several occasions that disclosing whether or not it has assisted the United States in connection with the Programs would violate federal law, including some laws that carry felony sanctions. For example, on June 14, 2006, in connection with the New Jersey Attorney General's effort to subpoena information relating to the alleged Calling Records Program, AT&T was advised in writing by the United States Department of Justice 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."⁶ Specifically, the United States directed AT&T that confirming or denying participation in the Programs would violate the National Security Agency Act of 1959, 18 U.S.C. § 798, and Executive Orders governing access to and handling of national security information.

³ See Press Conference of President Bush (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>.

⁴ See US Dept. of Justice, *Legal Authorities Supporting The Activities Of The National Security Agency Described By The President* (Jan. 19, 2006) <http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf>.

⁵ See Leslie Cauley, "NSA Has Massive Database of Americans' Phone" Calls, *USA Today*, May 11, 2006, at A1.

⁶ Letter from Assistant Attorney General Peter D. Keisler to Bradford A. Berenson *et al.* (Exhibit 2).

Board of Directors
AT&T Inc.
November 22, 2006
Page 3

Federal Criminal Prohibition On Disclosure Of Classified Information Concerning The Communication Intelligence Activities Of The United States. It is a felony under federal law to knowingly and willfully divulge to an unauthorized person classified information regarding the communications intelligence activities of the United States. In particular, 18 U.S.C. § 798(a) provides:

Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States, or for the benefit of any foreign government to the detriment of the United States any classified information –

* * * *

- (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or
- (3) concerning the communication intelligence activities of the United States or any foreign government . . .

* * * *

Shall be fined under this title or imprisoned not more than ten years, or both.

*Id.*⁷

⁷ As defined by this statute, 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. . . .” 18 U.S.C. § 798(b). The term “unauthorized person” means “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 to engage in communication intelligence activities for the United States.” *Id.*

Board of Directors
AT&T Inc.
November 22, 2006
Page 4

Disclosure of classified information pertaining to the Programs to any "unauthorized person," which would include members of the general public such as the Company's shareholders, would violate federal law and thereby subject the Company to potential criminal liability under this section. As Assistant Attorney General Peter D. Keisler, made clear to the former Attorney General of New Jersey, the Honorable Zulima V. Farber, regarding her attempt to investigate these same Programs,

It . . . 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.' . . . To the extent your subpoenas seek to compel disclosure of such information to state officials, responding to them would obviously violate federal law."⁸

Letter from Assistant Attorney General Peter Keisler to New Jersey Attorney General Zulima Farber, at 4 (June 14, 2006) (Exhibit 4).⁹

Other official government statements further confirm that any information relating to the Terrorist Surveillance Program beyond what the United States has publicly confirmed or any information at all concerning an alleged Calling Records Program would be classified, if such information exists. The Attorney General of the United States has personally noted that the Terrorist Surveillance Program is among the most highly classified programs in the entire

⁸ See also Section 6 of the National Security Agency Act, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note ("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, or of any information with respect to the activities thereof"); *Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996) ("[t]he protection afforded by section 6 is, by its very terms, absolute"); *Founding Church of Scientology v. National Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden v. National Security Agency*, 608 F.2d 1381, 1390 (D.C. Cir. 1979). When petitioned to investigate the Programs, the Federal Communications Commission declined to do so stating that "[t]he Commission has no power to order the production of classified information," and noting further that, because section 6 of the National Security Act of 1959 independently prohibits disclosure of information relating to NSA activities, the Commission lacks the authority to compel the production of the information necessary to undertake an investigation. See Letter from Kevin J. Martin, Chairman Federal Communications Commission to the Honorable Edward J. Markey, at 1-2 (May 22, 2006) (Exhibit 3).

⁹ See also 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>. ("This is a very classified program. It is probably the most classified program that exists in the United States government. . . .").

Board of Directors
AT&T Inc.
November 22, 2006
Page 5

government. 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>. (“This is a very classified program. It is probably the most classified program that exists in the United States government. . .”).

The United States, through the personal, sworn declaration of the Director of National Intelligence, has indeed formally identified much of the information called for by the Proposal, if such information exists, as classified. See Unclassified Declaration of the Honorable John D. Negroponete, ¶ 11 (Exhibit 5).¹⁰ As Director Negroponete stated, “[m]y assertion of the state secrets and statutory privileges in this case includes any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA.”). *Id.* ¶ 11.¹¹ As noted, the United States has formally directed that AT&T may not publicly disclose any responsive information concerning the claimed Programs. Furthermore, a recent decision of the United States District for the District of Columbia in *People for the American Way Foundation v. NSA et al.*, Civil Action No. 06-206 (ESH) (Nov. 20, 2006), held, pursuant to 5 U.S.C. § 552(b)(1), that even basic numerical or statistical information about the Terrorist Surveillance Program was and remains classified and therefore exempt from disclosure under the Freedom of Information Act. See slip op. at 14-18 (Exhibit 6). Although there are pending challenges to the scope of the United States’ state secrets assertion, we are aware of no

¹⁰ The Director of National Intelligence made his declaration relating to the Programs in the course of formally invoking the constitutionally-based state secrets doctrine, also known as the military and state secrets privilege (“state secrets privilege”). See *United States v. Reynolds*, 345 U.S. 1, 7 (1953). This privilege belongs exclusively to the federal government and protects any information which if disclosed 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). Given the significance of the privilege, the invocation of state secrets is made only formally through a personal declaration or 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); see also, e.g., *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

¹¹ The United States has repeatedly asserted this “state secrets privilege” with regard to the information that the Company would be required to disclose if the Proposal were implemented. For example, in *Terkel v. AT&T Corp.*, Case No. 06-cv-2837 (N.D. Ill.), the United States submitted the declaration of Director Negroponete, in which he concluded that “[e]ven confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection.” *Id.*

Board of Directors
AT&T Inc.
November 22, 2006
Page 6

challenges to the United States' assertion that information pertaining to the Programs is classified.¹²

The subjects covered by the criminal prohibition on disclosure of communications intelligence are thus the same subjects which the Proposal concerns. For instance, assuming *arguendo* that the Company participated in the Terrorist Surveillance Program or the Calling Records Program, notifying customers that their information had been shared as part of a Program would (1) confirm the existence of one or both Programs, (2) confirm AT&T's participation in one or both Programs, and (3) apprise targets of federal intelligence activities that they were the subject of surveillance by federal national security agencies. Likewise, detailing the expenditures made by the Company for the "operations" associated with these Programs would confirm their existence, confirm AT&T's participation in them, and furnish information concerning their scope.

Additional restrictions on disclosure. The Proposal further would require a report that would detail, among other things, specified information concerning all forms of "disclosure of the content of customer communications or records to the Federal Bureau of Investigation, NSA, and other government agencies without a warrant." MacKerron Letter (Exhibit 1). This implicates several other statutory prohibitions on disclosure.

First, although the alleged Programs underlying the Proposal are claimed by the Proponent to have occurred outside the statutory regime established by the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 et seq., the terms of the Proposal would require disclosure of any FISA surveillance. 50 U.S.C. § 1802(a)(4) provides that where electronic surveillance occurs pursuant to FISA without any type of court order (as it may under certain circumstances), a carrier may be directed by the Attorney General to protect the secrecy of such surveillance and adhere to prescribed security procedures to ensure that is done, and the carrier must comply with that directive. The same is true for electronic surveillance accomplished pursuant to a FISA order, which does not constitute a conventional "warrant" issued upon probable cause within the meaning of the Proposal. *See id.* §§ 1805(c)(2)(B) & (C).

Furthermore, pursuant to 50 U.S.C. § 1861, the Federal Bureau of Investigation is authorized to obtain customer information from telecommunications carriers upon application to

¹² As you are aware, we represent AT&T Inc. and affiliated entities in MDL 06-1791 VRW: *In re National Security Agency Telecommunications Records Litigation* and related cases. As you are also aware, we have no financial interest in the outcome of that litigation. Although we have briefed and argued various legal issues related to the Programs during the course of MDL 1791 and related cases, we base this Opinion solely on the analysis presented herein. It should be understood that this Opinion does not, and should not be construed to, predict the outcome of any pending litigation.

Board of Directors
AT&T Inc.
November 22, 2006
Page 7

a court for a FISA order but without a conventional warrant. When such business records are produced, the carrier is prohibited from disclosing "to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section," subject to certain exceptions not applicable here. *Id.* § 1861(d).

Finally, under applicable provisions of the Stored Communications Act, the Director of the FBI is authorized to demand and obtain from a wire or electronic communication service provider transactional, billing, or calling records without any form of court order, and in many circumstances, the carrier is categorically barred from disclosing receipt or fulfillment of such a request, again subject to exceptions not applicable here. *See* 18 U.S.C. § 2709(c).

The Proposal would require the disclosure of information in each of the above categories, to the extent such information exists.

Opinion. Based on the foregoing facts and analysis regarding the Proposal as recited herein, and subject to the qualifications, assumptions and discussion contained herein, we are of the opinion that the Proposal would, if implemented, cause the AT&T to violate one or more federal laws to which it is subject.¹³

Very truly yours,

SIDLEY AUSTIN LLP

Sidley Austin LLP

¹³ Our analysis is limited to the facts and assumptions as they are presented herein and is subject to the qualification that there are no additional facts that would materially affect the validity of the assumptions and conclusions set forth herein or upon which this opinion is based. Our conclusions are based on the law specifically referenced here as of the date hereof, we express no opinion as to the laws, rules or regulations not specifically referenced, and we assume no obligation to advise you of changes in the law or fact (or the effect thereof on the Opinion expressed or the statements made herein) that hereafter may come to our attention. Our opinions are limited to the specific opinions expressed in this "Opinion" section. The foregoing assessment is not intended to be a guarantee as to what a particular court would actually hold, but an assessment of a reviewing court's action if the issues were properly presented to it and the court followed what we believe to be the applicable legal principles. This opinion may not be relied upon in whole or in part by any other person or entity other than its addressee without our specific prior written consent. We understand that you intend to attach a copy of this opinion to your letter relating to the Proposal to the Securities & Exchange Commission under the procedures set forth in 17 CFR 240.14a-8, and we hereby consent to the use of this opinion for that purpose.

EXHIBIT 1



311 California Street, Suite 510
San Francisco, CA 94104
T 415.391.3212
F 415.391.3245
www.asyousow.org

Oct. 24, 2006

Edward E. Whitacre
CEO
AT&T Inc.
175 E. Houston
San Antonio, TX 78205

Dear Mr. Whitacre:

As You Sow is a non-profit organization whose mission is to promote corporate accountability. We represent Mr. Jeremy Kagan, a shareholder of AT&T stock.

We are concerned about reports that AT&T provided customer information to the National Security Agency without a warrant. We believe this action may have compromised customer privacy protections. Further, it could affect AT&T's reputation and good standing. This alleged program has resulted in numerous press stories on the subject and the filing of many lawsuits against the company. It is important for the company to report to stockholders on legal and ethical issues surrounding disclosure of the content of customer communications to federal authorities without a warrant, as well as the impact this action may have on our customers. It could also have an impact on the share price which may be affected by potential legal liabilities.

Therefore, we are submitting the enclosed shareholder proposal for inclusion in the 2007 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities Exchange Act of 1934.

Proof of ownership and authorization to act for Mr. Kagan is attached. The shareholder will continue to hold the shares through the 2007 stockholder meeting. A representative of the filer will attend the stockholders' meeting to move the resolution. Mr. Kagan, represented by As You Sow, is the primary filer of this proposal. Other stockholders will be co-filing this proposal under separate cover.

Please contact me if you would like to discuss this filing.

Sincerely,

A handwritten signature in black ink, appearing to read 'Conrad MacKerron', with a long horizontal flourish extending to the right.

Conrad B. MacKerron
Director, Corporate Social Responsibility Program

Enclosures



AT&T -- PRIVACY RIGHTS PROTECTION REPORT

WHEREAS: The right to privacy is a long established value, enshrined in the Constitution and decades of U.S. jurisprudence, and cherished by people of all political persuasions; and

Privacy protections serve many important societal purposes: encouraging development of science and knowledge; preventing fraud; and allowing individuals to communicate sensitive information (i.e. health care providers, clergy, brokers); and

AT&T's reputation and good standing may be placed in jeopardy by reports that it has voluntarily provided customer phone records and communications data to the National Security Agency, as first revealed by *USA Today*; and

We believe this alleged practice is seen by millions of Americans, including customers, shareholders and employees of AT&T, as a violation of our customers' privacy expectations and basic right to have phone and e-mail records kept confidential; and

This is an opportunity for our company to take an industry leadership role as a defender of privacy rights and thereby attract new customers. Our customers have the choice to go to other telecommunications companies if they do not agree with the company's practices and may do so. These events could affect, both positively and negatively, the long-term value of our company; and

This alleged program, as described in the *USA Today* report, has resulted in thousands of media stories on the subject and the filing of dozens of lawsuits against AT&T. These cases were brought not only by the American Civil Liberties Union and Electronic Frontier Foundation, but by our own customers in consumer class actions, seeking billions of dollars in damages; and

These allegations pose questions in regard to general respect for the rule of law upon which our democratic system depends; and

In light of the potentially negative uses of today's technology, we believe it is important that AT&T re-examine the steps it takes to protect the values embodied in an individual's right to privacy.

RESOLVED: That shareholders request that the Board of Directors issue a report to shareholders in six months, at reasonable cost and excluding confidential and proprietary information, which describes the following:

- The overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies;
- Any additional policies, procedures or technologies AT&T could implement to further ensure (a) the integrity of customers' privacy rights and the confidentiality of customer information, and (b) that customer information is only released when required by law; and
- AT&T's past expenditures on attorney's fees, experts fees, operations, lobbying and public relations/media expenses, relating to this alleged program.

SUPPORTING STATEMENT

We believe it will benefit society, our customers, shareholders and AT&T's long-term value for the company to take a leadership role as protector of privacy rights and to issue this report. The proponents urge a YES vote.

EXHIBIT 2



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

June 14, 2006

VIA FACSIMILE AND EMAIL

Bradford A. Berenson, Esq.
Sidley Austin LLP
1501 K Street, NW
Washington, D.C. 20005

John A. Rogovin, Esq.
Wilmer Hale
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006

John G. Kester, Esq.
Williams & Connolly LLP
725 Twelfth Street, NW
Washington, D.C. 20005

Christine A. Varney, Esq.
Hogan & Hartson LLP
555 Thirteenth Street, NW
Washington, D.C. 20004

**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 Counsel:

This letter is to advise you that today the United States of America has filed a lawsuit against the Attorney General and other officials of the State of New Jersey, as well as AT&T Corp., Verizon Communications, Inc., Qwest Communications International, Inc., Sprint Nextel Corporation, and Cingular Wireless LLC (together the "telecommunications carriers"). That lawsuit seeks a declaration that those state officials do not have the authority to enforce subpoenas duces tecum (hereafter the "subpoenas") recently issued to the telecommunications carriers seeking information relating to the alleged provision of "telephone call history data" to the National Security Agency, and that the telecommunications carriers cannot respond to these subpoenas. A copy of the Complaint the United States has filed, as well as a letter we have sent today to Attorney General Farber, are attached hereto.

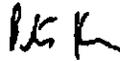
As noted in our Complaint and letter to Attorney General Farber concerning those issues, the subpoenas infringe upon federal operations, are contrary to federal law, and are invalid under the Supremacy Clause of the United States Constitution. Responding to the subpoenas – including by disclosing whether or to what extent any responsive materials exist – would violate federal laws and Executive Orders. Moreover, the Director of National Intelligence recently has asserted the state secrets privilege with respect to the very same topics and types of information sought by the subpoenas, thereby underscoring that any such information cannot be disclosed. For these reasons, described in more detail in the attachments hereto, please be advised that we

Messrs. Berenson, Kester, Rogovin, Ms. Varney
Page 2

believe that enforcing compliance with, or responding to, the subpoenas would be inconsistent with and preempted by federal law.

Please do not hesitate to contact Carl Nichols or me should you have any questions in this regard.

Sincerely,



Peter D. Keisler
Assistant Attorney General

Attachments

EXHIBIT 3



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

May 22, 2006

The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications and the Internet
Energy and Commerce Committee
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding recent media reports concerning the collection of telephone records by the National Security Agency. In your letter, you note that section 222 of the Communications Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." 47 U.S.C. § 222(a). You have asked me to explain the Commission's plan "for investigating and resolving these alleged violations of consumer privacy."

I know that all of the members of this Commission take very seriously our charge to faithfully implement the nation's laws, including our authority to investigate potential violations of the Communications Act. In this case, however, the classified nature of the NSA's activities makes us unable to investigate the alleged violations discussed in your letter at this time.

The activities mentioned in your letter are currently the subject of an action filed in the United States District Court for the Northern District of California. The plaintiffs in that case allege that the NSA has "arrang[ed] with some of the nation's largest telecommunications companies . . . to gain direct access to . . . those companies' records pertaining to the communications they transmit." *Hepting v. AT&T Corp.*, No. C-06-0672-VRW (N.D. Cal.), Amended Complaint ¶ 41 (Feb. 22, 2006). According to the complaint, for example, AT&T Corp. has provided the government "with direct access to the contents" of databases containing "personally identifiable customary proprietary network information (CPNI)," including "records of nearly every telephone communication carried over its domestic network since approximately 2001, records that include the originating and terminating telephone numbers and the time and length for each call." *Id.* ¶¶ 55, 56, 61; *see also, e.g.*, Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today* A1 (May 11, 2006) (alleging that the NSA "has been secretly collecting the phone call records of tens of millions of Americans, using data provided" by major telecommunications carriers).

The government has moved to dismiss the action on the basis of the military and state secrets privilege. *See Hepting, Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America* (May 12, 2006). Its motion is accompanied by declarations from John D. Negroponte, Director of National Intelligence, and Lieutenant General Keith B. Alexander, Director, National Security Agency, who have maintained that disclosure of information “implicated by Plaintiffs’ claims . . . could reasonably be expected to cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶ 9. They specifically address “the NSA’s purported involvement” with specific telephone companies, noting that “the United States can neither confirm nor deny alleged NSA activities, relationships, or targets,” because “[t]o do otherwise when challenged in litigation would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general.” Alexander Decl. ¶ 8.

The representations of Director Negroponte and General Alexander make clear that it would not be possible for us to investigate the activities addressed in your letter without examining highly sensitive classified information. The Commission has no power to order the production of classified information. Rather, the Supreme Court has held that “the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment.” *Department of the Navy v. Egan*, 484 U.S. 518, 529 (1988).

The statutory privilege applicable to NSA activities also effectively prohibits any investigation by the Commission. The National Security Act of 1959 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 [or] of any information with respect to the activities thereof.” Pub. L. No. 86-36, § 6(a), 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note. As the United States Court of Appeals for the District of Columbia Circuit has explained, the statute’s “explicit reference to ‘any other law’ . . . must be construed to prohibit the disclosure of information relating to NSA’s functions and activities as well as its personnel.” *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996); *see also Hayden v. NSA/Central Sec. Serv.*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (“Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.”). This statute displaces any authority that the Commission might otherwise have to compel, at this time, the production of information relating to the activities discussed in your letter.

Page 3—The Honorable Edward J. Markey

I appreciate your interest in this important matter. Please do not hesitate to contact me if you have further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin J. Martin". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Kevin J. Martin
Chairman

EXHIBIT 4



U. S. Department of Justice

Civil Division

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

The Honorable Zulima V. Farber
Page 2

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 authority² 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."

The Honorable Zulima V. Farber
Page 3

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 *Garamendi*, 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.

The Honorable Zulima V. Farber

Page 4

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).

The Honorable Zulima V. Farber
Page 5

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," Negroponce 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 Negroponce 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." Negroponce Decl. ¶12; *see also* Alexander Decl. ¶8. As DNI Negroponce 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." Negroponce 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 Honorable Zulima V. Farber
Page 6

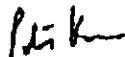
the DNI's authority and the Act of Congress conferring that authority. More broadly, the subpoenas involve an improper effort to use state law to regulate or oversee federal functions, and implicate federal immunity under the Supremacy Clause.

* * *

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

EXHIBIT 5

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

STUDS TERKEL, BARBARA FLYNN CURRIE,)
DIANE C. GERAGHTY, GARY S. GERSON)
JAMES D. MONTGOMERY, and QUENTIN)
YOUNG, on behalf of themselves and all others)
similarly situated, and the AMERICAN CIVIL)
LIBERTIES UNION OF ILLINOIS,)

Case No. 06 C 2837

Hon. Matthew F. Kennelly

Plaintiffs,)

v.)

AT&T INC., AT&T CORP., and ILLINOIS)
BELL TELEPHONE CO. d/b/a AT&T ILLINOIS,)

Defendants.)

**DECLARATION OF JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL INTELLIGENCE**

I, John D. Negroponte, declare as follows:

INTRODUCTION

1. I am the Director of National Intelligence (DNI) of the United States. I have held this position since April 21, 2005. From June 28, 2004, until appointed to be DNI, I served as the United States Ambassador to Iraq. From September 18, 2001, until my appointment in Iraq, I served as the United States Permanent Representative to the United Nations. I have also served as Ambassador to Honduras (1981-1985), Mexico (1989-1993), the Philippines (1993-1996), and as Deputy Assistant to the President for National Security Affairs (1987-1989).

2. In the course of my official duties, I have been advised of this lawsuit and the allegations at issue in this case. The statements made herein are based on my personal knowledge, as well as on information provided to me in my official capacity as DNI, and on my

personal evaluation of that information. In personally considering this matter, I have executed a separate classified declaration dated June 30, 2006, and lodged *in camera* and *ex parte* in this case. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte Declaration* of Lieutenant General Keith B. Alexander, Director of the National Security Agency, lodged in this case.

3. The purpose of this declaration is to formally assert, in my capacity as DNI and head of the United States Intelligence Community, the military and state secrets privilege (hereafter "state secrets privilege"), as well as a statutory privilege under the National Security Act, *see* 50 U.S.C. § 403-1(i)(1), in order to protect certain intelligence-related information implicated by the allegations in this case. Disclosure of the information covered by these privilege assertions would cause exceptionally grave damage to the national security of the United States and, therefore, should be excluded from any use in this case. In addition, I concur with General Alexander's conclusion that the risk is great that further litigation will lead to the disclosure of information harmful to the national security of the United States and, accordingly, this case should be dismissed.

THE DIRECTOR OF NATIONAL INTELLIGENCE

4. The position of Director of National Intelligence was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of the Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the U.S. Intelligence Community and as the principal advisor to the President, the National Security Council, and the Homeland Security Council, for intelligence-related matters related to national security. *See* 50 U.S.C. § 403(b)(1), (2).

5. The "United States Intelligence Community" includes the Office of the Director

of National Intelligence; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the military services, the Federal Bureau of Investigation, the Department of Treasury, the Department of Energy, Drug Enforcement Administration, and the Coast Guard; the Bureau of Intelligence and Research of the Department of State; the elements of the Department of Homeland Security concerned with the analysis of intelligence information; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and heads of the department or agency concerned, as an element of the Intelligence Community. *See* 50 U.S.C. § 401a(4).

6. The responsibilities and authorities of the DNI are set forth in the National Security Act, as amended. *See* 50 U.S.C. § 403-1. These responsibilities include ensuring that national intelligence is provided to the President, the heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1). The DNI is also charged with establishing the objectives of, determining the requirements and priorities for, and managing and directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the Intelligence Community. *Id.* § 403-1(f)(1)(A)(i) and (ii). The DNI is also responsible for developing and determining, based on proposals submitted by heads of agencies and departments within the Intelligence Community, an annual consolidated budget for the National Intelligence Program for presentation to the President, and for ensuring the effective execution of the annual budget for intelligence and intelligence-related activities, and for managing and allotting appropriations for the National

Intelligence Program. *Id.* § 403-1(c)(1)-(5).

7. In addition, the National Security Act of 1947, as amended, provides that “The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI establishes and implements guidelines for the Intelligence Community for the classification of information under applicable law, Executive Orders, or other Presidential directives and access and dissemination of intelligence. *Id.* § 403-1(i)(2)(A), (B). In particular, the DNI is responsible for the establishment of uniform standards and procedures for the grant of access to Sensitive Compartmented Information (“SCI”) to any officer or employee of any agency or department of the United States, and for ensuring consistent implementation of those standards throughout such departments and agencies. *Id.* § 403-1(j)(1), (2).

8. By virtue of my position as the DNI, and unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. Pursuant to Executive Order No. 12958, 3 C.F.R. § 333 (1995), as amended by Executive Order 13292 (March 25, 2003), reprinted as amended in 50 U.S.C.A. § 435 at 93 (Supp. 2004), the President has authorized me to exercise original TOP SECRET classification authority. My classified declaration, as well as the classified declaration of General Alexander on which I have relied in this case, are properly classified under § 1.3 of Executive Order 12958, as amended, because the public disclosure of the information contained in those declarations could reasonably be expected to cause exceptionally grave damage to national security of the United States.

ASSERTION OF THE STATE SECRETS PRIVILEGE

9. After careful and actual personal consideration of the matter, I have determined that the disclosure of certain information implicated by Plaintiffs’ claims—as set forth here and

described in more detail in my classified declaration and in the classified declaration of General Alexander—would cause exceptionally grave damage to the national security of the United States and, therefore, such information must be protected from disclosure and excluded from this case. Accordingly, as to this information, I formally invoke and assert the state secrets privilege. In addition, it is my judgment that any attempt to proceed in the case will substantially risk the disclosure of the privileged information described briefly herein and in more detail in the classified declarations, and will cause exceptionally grave damage to the national security of the United States.

10. Through this declaration, I also invoke and assert a statutory privilege held by the DNI under the National Security Act to protect intelligence sources and methods implicated by this case. *See* 50 U.S.C. § 403-1(i)(1). My assertion of this statutory privilege for intelligence information and sources and methods is coextensive with my state secrets privilege assertion.

INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE

11. My assertion of the state secrets and statutory privileges in this case includes any information tending to confirm or deny (a) alleged intelligence activities, such as the alleged collection by the NSA of records pertaining to a large number of telephone calls, (b) an alleged relationship between the NSA and AT&T (either in general or with respect to specific alleged intelligence activities), and (c) whether particular individuals or organizations have had records of their telephone calls disclosed to the NSA. My classified declaration describes in further detail the information over which I assert privilege.

12. As a matter of course, the United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets. The harm of revealing such information should be obvious. If the United States confirms that it is conducting a particular intelligence activity, that it is gathering information from a particular source, or that

it has gathered information on a particular person, such intelligence-gathering activities would be compromised and foreign adversaries such as al Qaeda and affiliated terrorist organizations could use such information to avoid detection. Even confirming that a certain intelligence activity or relationship does *not* exist, either in general or with respect to specific targets or channels, would cause harm to the national security because alerting our adversaries to channels or individuals that are not under surveillance could likewise help them avoid detection. In addition, denying false allegations is an untenable practice. If the government, for example, were to confirm in certain cases that specific intelligence activities, relationships, or targets do not exist, but then refuse to comment (as it would have to) in a case involving an actual intelligence activity, relationship, or target, a person could easily deduce by comparing such responses that the latter case involved an actual intelligence activity, relationship, or target. Any further elaboration on the public record concerning these matters would reveal information that would cause the very harms that my assertion of privilege is intended to prevent. The classified declaration of General Alexander that I considered in making this privilege assertion, as well as my own separate classified declaration, provide a more detailed explanation of the information at issue and the harms to national security that would result from its disclosure.

13. The information covered by my privilege assertion includes, but is not limited to, any such information necessary to respond to Plaintiffs' First Amended Complaint, Plaintiffs' Motion for a Preliminary Injunction, or Plaintiffs' First Set of Interrogatories.

CONCLUSION

14. In sum, I formally assert the state secrets privilege, as well as a statutory privilege under the National Security Act, 50 U.S.C. § 403-1(i)(1), to prevent the disclosure of the information described herein and in my classified declaration, as well as General Alexander's classified declaration. Moreover, because the very subject matter of this lawsuit concerns alleged intelligence activities, the litigation of this case directly risks the disclosure of privileged intelligence-related information. Accordingly, I join with General Alexander in respectfully requesting that the Court dismiss this case to stem the harms to the national security of the United States that will occur if such information is disclosed.

I declare under penalty of perjury that the foregoing is true and correct.

DATE: _____

6/30/06

John Negroponte

JOHN D. NEGROPONTE
Director of National Intelligence

EXHIBIT 6

BACKGROUND

The NSA is a separate agency within the Department of Defense charged with collecting, processing and disseminating signals intelligence ("SIGINT") information for foreign intelligence purposes, along with other objectives relating to national security. (Def.'s Facts ¶¶ 1, 2.) In the aftermath of September 11, 2001, President Bush authorized the NSA to intercept the international communications to and from the United States of people linked to al Qaeda or related terrorist organizations. (Def. Mot. at 5.) This surveillance was conducted without obtaining a warrant from the Foreign Intelligence Surveillance Court. (Pl. Mot. at 2.) The existence of this previously secret program -- known as the TSP -- was first acknowledged by President Bush on December 17, 2005. (Def.'s Facts ¶ 17.) Senate testimony by General Michael Hayden, current director of the Central Intelligence Agency and former director of the NSA, and similar statements from other government officials, indicate that lawyers from the United States Department of Justice and the White House Counsel's office have been involved in analyzing the legality of the TSP. (Pl. Mot. at 21; Def. Reply at 14.)

On December 29, 2005, plaintiff, a non-profit public interest organization whose stated mission is to educate the general public regarding current issues of civil and constitutional rights (Compl. ¶ 4), submitted a FOIA request to the NSA seeking records relating to the TSP. (Def.'s Facts ¶ 22.) Plaintiff then filed this action on February 6, 2006, to compel release of the requested records. (Compl. ¶ 1.) Plaintiff's original FOIA request sought sixteen categories of documents, but plaintiff has since withdrawn eleven of these specific requests.^{1/} (Pl. Mot. at 1.)

^{1/}On February 14, 2006, defendant produced 106 pages of documents responsive to one of plaintiff's withdrawn requests, and explained that it had no documents responsive to several other of the withdrawn requests. (Def.'s Facts ¶ 24.)

Five of the original document requests remain at issue here. Specifically, plaintiff seeks:

- No. 2: Any and all documents that refer, reflect or relate to the total number of individuals that have been the subject of electronic surveillance by the NSA in the United States without a court approved warrant pursuant to [President Bush's Executive] Order since the date of the Order up to the date of this request.
- No. 3: Any and all documents that refer, reflect or relate to the total number of individuals who have been the subject of warrantless electronic surveillance by the NSA in the United States since the mid-2004 Department of Justice audit of the NSA's warrantless domestic electronic surveillance program up to the date of this request.
- No. 4: Any and all documents that refer, reflect or relate to the total number of wiretaps or other instances of electronic surveillance conducted by the NSA pursuant to authority granted the NSA by the Order regardless of whether such number includes successive wiretaps conducted on the same individual.
- No. 6: Any and all documents relating to any audit or review of the NSA's program to conduct domestic warrantless electronic surveillance on individuals within the United States . . . pursuant to the Order since its execution, whether such audit or review was conducted internally by the NSA or externally, and whether such review or audit was conducted for the benefit of congressional or executive branch use.
- No. 16: Any and all NSA records relating to People For the American Way Foundation or People for the American Way.

(Pl. Ex. 1 [Dec. 29, 2005 FOIA Request] at 1-3.) As an alternative to its requests 2-4, plaintiff states that it would "accept a full list of the domestic wiretaps or other electronic surveillance conducted by the NSA and the number of persons subject to that surveillance within the requested time frame under the authority granted by the Order, with the names of the targeted individuals and organizations redacted." (*Id.* at 3.)

Citing FOIA Exemptions 1, 3 and 5, defendant has withheld documents responsive to

requests 2-4 and 6, and has refused to confirm or deny the existence of documents responsive to request 16. (Def.'s Facts ¶ 24; Def Mot. at 10, 17, 34.) Defendant has filed the declarations of two NSA officials explaining the agency's reasons for the withholdings. (See Declaration of Louis F. Giles; Declaration of Joseph B.; Supplemental Declaration of Louis F. Giles.) According to these declarations, documents responsive to requests 2-4 and 6 relate to the sensitive activities and functions of the NSA, and their disclosure could reasonably be expected to cause grave damage to national security. (Joseph B. Decl. ¶¶ 9, 10, 14, 18, 19.) This information, defendant argues, is exempt from disclosure because it is protected by several federal statutes, and also because it has been properly classified "TOP SECRET-SCI"^{2/} pursuant to executive order. (See *id.* ¶¶ 14, 15, 19.) The declarations also explain that the NSA cannot, in the interest of national security, confirm or deny the existence of records responsive to request 16, because confirmation or denial of the NSA's surveillance of any particular target "would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities and methods." (*Id.* ¶ 27.) Thus, defendant claims, the fact of the existence or nonexistence of documents responsive to request 16 is also properly classified and protected from disclosure by federal statute, and therefore is exempt from disclosure under FOIA. (*Id.* ¶¶ 28-29.) Based on these declarations, defendant has moved for summary judgment on all of plaintiff's outstanding requests.

^{2/} Information is classified as "Sensitive Compartment Information" ("SCI") when it "involves or derives from particularly sensitive intelligence sources and methods." (Joseph B. Decl. ¶ 4.) Access to such information "requires clearance beyond the 'Top Secret' level" and is "required to be handled exclusively within formal access control systems established by the Director of [National] Intelligence." *Guillot v. Garrett*, 970 F.2d 1320, 1322 n. 1 (4th Cir. 1992).

Plaintiff has likewise moved for summary judgment on its requests 2-4, and opposes defendant's motion for summary judgment with respect to requests 6 and 16. (Pl. Mot. at 1.) In support of its motion, plaintiff argues that defendant's declarations are insufficient to support defendant's withholdings under FOIA. (*See id.* at 5.) Specifically, with respect to requests 2-4, plaintiff contends that the disclosure of "bare statistics" regarding the total number of individuals and communications subject to NSA surveillance could not reasonably be expected to result in damage to the national security, and that it would not reveal anything about the NSA's sources, methods, or procedures, nor expose any function of the NSA that is not already known to the public. (*Id.* at 6, 11, 14-17.) Similarly, plaintiff argues that confirming or denying the existence of records responsive to request 16 -- information relating solely to any surveillance of plaintiff's own communications under the TSP-- would not cause harm cognizable under any FOIA exemption, as it relates to only one of "hundreds of millions" of potential surveillance targets and would not reveal anything about the millions of other potential targets. (*Id.* at 27, 30.) Regarding request 6, plaintiff argues that the request encompasses any "legal opinions" concerning the TSP, and that defendant failed to justify the exemption of such documents in their entirety in reasonably specific detail. (*Id.* at 21.) Finally, citing a recent district court decision from another jurisdiction that held the TSP to be illegal and unconstitutional, plaintiff argues that none of FOIA's exemptions applies to its requests for information about the TSP because "FOIA . . . cannot and should not be used as a method of shielding illegal government activity." (Pl. Reply at 4.)

ANALYSIS

I. Standard of Review under FOIA

Under FOIA, an agency must disclose all records requested by any person unless the agency can establish that the information falls within one of the nine exemptions set forth in the statute. See 5 U.S.C. §§ 552(a)(3)-(b). These exemptions are exclusive, and should be narrowly construed. *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976). However, the Supreme Court has noted that the exemptions must be construed "to have a meaningful reach and application." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989). An agency that withholds information pursuant to one of these exemptions bears the burden of justifying its decision, and challenges to an agency's decision to withhold information are reviewed *de novo* by the district court. See 5 U.S.C. § 552(a)(4)(B); *King v. U.S. Dep't of Justice*, 830 F.2d 210, 217 (D.C. Cir. 1987). At the same time, it is "well established that the judiciary owes some measure of deference to the executive in cases implicating national security, a uniquely executive purview." *Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice*, 331 F.3d 918, 926-27 (D.C. Cir. 2003) (citing *Zadvydas v. Davis*, 533 U.S. 678, 696 (2001) (noting that "terrorism or other special circumstances" might warrant "heightened deference to the judgments of the political branches"))).

Summary judgment may be granted to the government in a FOIA case if "the agency proves that it has fully discharged its obligations under the FOIA, after the underlying facts and the inferences to be drawn from them are construed in the light most favorable to the FOIA requester." *Greenberg v. U.S. Dep't of Treasury*, 10 F. Supp. 2d 3, 11 (D.D.C. 1998) (citation omitted). The Court may award summary judgment solely on the information provided in

affidavits or declarations when they describe “the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.” *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981) (citations omitted); *see also Vaughn v. Rosen*, 484 F.2d 820, 826 n.20 (D.C. Cir. 1973) (citing *EPA v. Mink*, 410 U.S. 73, 93 (1973)). Summary judgment is not warranted if the declarations are “conclusory, merely reciting statutory standards, or . . . too vague or sweeping.” *King*, 830 F.2d at 219 (internal quotation marks and citation omitted).

Applying these standards, the Court finds that defendant’s declarations are sufficiently detailed and specific and that they justify the withholding of the information at issue. The Court therefore upholds defendant’s invocation of Exemptions 1 and 3.^{2/}

II. Exemption 3

Defendant claims that the requested documents are shielded from disclosure under FOIA Exemption 3, which provides for nondisclosure of matters that are “specifically exempted from disclosure by statute” 5 U.S.C. § 552(b)(3). Exemption 3 applies if the statute in question “(A) requires that matters be withheld from the public in such a manner as to leave no discretion on the issues, and (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.” *Id.* In other words, defendant must point to an appropriate nondisclosure statute, and must demonstrate that the withheld materials are covered by that particular statute. *See CIA v. Sims*, 471 U.S. 159, 167 (1985). Here, defendant claims exemption

^{2/}Because either Exemption 1 or 3 provides a valid basis for granting defendant’s motion for summary judgment, the Court need not address defendant’s claim under Exemption 5.

from FOIA under three separate statutes: (1) Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63, *codified at* 50 U.S.C. § 402 note; (2) Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638, *codified at* 50 U.S.C. § 403-1(i)(1); and (3) 18 U.S.C. § 798. (Def. Mot. at 11-13.) Courts have held, and plaintiff does not dispute, that each of these three statutes qualify under FOIA Exemption 3. *See Larson v. Dep't of State*, No. 02-1937, 2005 WL 3276303, at *19 (D.D.C. Aug. 10, 2005), *appeal docketed* No. 06-5112 (D.C. Cir. Apr. 21, 2006).

Section 6 of the NSA Act of 1959 is the broadest of the three statutes cited by defendant.

It provides:

[N]othing 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, [or] of any information with respect to the activities thereof

50 U.S.C. § 402 note. As the D.C. Circuit has explained, “[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. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996); *see Fitzgibbon v. CIA*, 911 F.2d 755, 761-62 (D.C. Cir. 1990) (“Exemption 3 differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within the statute’s coverage.” (quoting *Ass’n. of Retired R.R. Workers v. U.S. R.R. Ret. Bd.*, 830 F.2d 331, 336 (D.C. Cir. 1987)) (internal quotation marks omitted)). However, “[b]arren assertions that an exempting statute has been met cannot suffice to establish that fact” *Founding Church of Scientology of Wash., D.C., Inc. v. NSA*, 610 F.2d 824, 831 (D.C. Cir. 1979).

The declaration of Joseph B., who oversees the SIGINT operations of the NSA, states that the NSA has a number of documents responsive to plaintiff's requests 2-4, consisting of "briefing slides" that "detail information related to the number of individuals subject to surveillance, contain the identity of some individuals, and contain information related to the number of communications intercepted under the TSP." (Decl. of Joseph B. ¶¶ 1, 9.) The declarant explains that the disclosure of such statistics relating to the operation of the TSP "would reveal information about NSA's success or lack of success in implementing the TSP," as well as "information about the U.S. intelligence community's capabilities, priorities, and activities." (*Id.* ¶ 12.) Accordingly, he contends, information responsive to requests 2-4 relates to "the NSA's activities and functions, and, more broadly, the sources and methods used by the intelligence community." (*Id.* ¶ 15.)

The Joseph B. declaration also acknowledges that the NSA possesses documents responsive to request 6, relating to "any audit or review" of the TSP. (*Id.* ¶ 18.) The declarant states that the responsive documents pertain to "the operation of the program, and provid[e] recommendations and suggestions for the effective operation of the program."⁴ (*Id.*) Further, he

⁴ Plaintiff contends that its request would "logically include" determinations about the legality of the TSP, and that any unclassified material regarding the TSP's legality must be produced. (Pl. Mot. at 19, 20.) Defendant acknowledges that such legal analysis and opinions exist, but maintains that plaintiff's request for "[a]ny and all documents relating to any audit or review" of the TSP, read in the context of its other requests, could not reasonably be interpreted to include *legal* determinations or opinions. (Def. Reply at 13-14.) Defendant interpreted plaintiff's request to involve information regarding "operational reviews" of the program. (*Id.*) The Court agrees that plaintiff's December 29, 2005 letter failed to ask for "documents reflecting outside determinations about the legality of the program," so the Court is unwilling to interpret plaintiff's request to include such legal opinions.

explains that because all of the material in these documents "is so intertwined with . . . information regarding the details of operation of the program" -- such as the dates, scope and effectiveness of the TSP -- that "no segregable portion of the responsive documents may be disclosed" under Section 6 and the other cited exemptions statutes. (*Id.* ¶ 20.)

Finally, with respect to plaintiff's request 16, which seeks any NSA records related to the surveillance of plaintiff, the NSA declines to confirm or deny the existence of responsive records. (*Id.* ¶ 27.) An agency's refusal to confirm or deny the existence of records is commonly known as a "Glomar response," see *Phillippi v. CIA*, 546 F.2d 1009 (D.C. Cir. 1976), and is proper when "to confirm or deny the existence of records . . . would cause harm cognizable under an FOIA exception." *Gardels v. CIA*, 689 F.2d 1100, 1103 (D.C. Cir. 1982). The NSA's declarations explain that "[c]onfirmation by NSA that a person's activities are not of foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities on a case-by-case basis would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods." (Decl. of Joseph B. ¶ 27.) The declarant further explains that "if NSA were to admit publicly in response to an information request that no information about Persons X, Y or Z exists, but in response to a separate information request about Person T state only that no response could be made, this would give rise to the inference that Person T is a target of the TSP." (*Id.*) This, it follows, would reveal information about the NSA's "organization, functions, and activities." (*Id.* ¶ 29.)

The Court is satisfied that defendant's declarations have described the withheld documents and information in a reasonably specific fashion and have put forth a rational

explanation for their withholding under Section 6 and Exemption 3. The NSA has averred that all the requested information concerns a specific NSA activity -- intelligence gathering based on "the collection of electronic communications" (Joseph B. Decl. ¶ 5) -- and has logically explained that the disclosure of this material would reveal information related to that NSA activity.³ See *Hayden v. NSA*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (holding that NSA documents obtained through monitoring foreign electromagnetic signals were exempt from FOIA disclosure under Section 6).

In response, plaintiff has failed to rebut defendant's explanations, nor does plaintiff even appear to contest that the information it requests relates to the NSA's SIGINT activities. (See Pl. Mot. at 16.) Instead, in the face of the formidable statutory hurdle presented by Section 6, plaintiff essentially asks the Court to evaluate the potential harm that would result from the disclosure of the requested information, contending that "the NSA's own characterization of its activities does not explain how they are so 'fragile' as to preclude the disclosure of the total number of individuals and communications subject to the NSA's secret surveillance program." (Pl. Mot. at 16.) As explained above, the law regarding Section 6 does not require the NSA to demonstrate what harm might result from the disclosure of its activities. "A specific showing of potential harm to national security . . . is irrelevant to the language of [Section 6]. Congress has

³In a typical FOIA case, the agency invoking the FOIA exemptions must provide the FOIA requester with a document index, known as a "*Vaughn* index," that itemizes each withheld document and the reasons for its withholding. See *Vaughn*, 484 F.2d at 827-28. In its declarations, the NSA explains that "because of the highly sensitive nature of the information involved" in this case, such an index would itself reveal classified information protected by FOIA Exemptions 1 and 3. (Giles Decl. ¶ 15.) Thus, a *Vaughn* index is not required here, where it "could cause the very harm that section 6 was intended to prevent." *Linder*, 94 F.3d at 697 (holding that no *Vaughn* index was required of SIGINT materials withheld by the NSA).

already, in enacting the statute, decided that the disclosure of NSA activities is potentially harmful.” *Hayden*, 608 F.2d at 1390; see *Linder*, 94 F.3d at 696.

Plaintiff also cites to dicta from the D.C. Circuit’s opinion in *Hayden v. NSA*, wherein the Court qualified its expansive interpretation of Section 6 by stating that “where the function or activity is *authorized by statute and not otherwise unlawful*, NSA materials integrally related to that function or activity fall within [Section 6] and Exemption 3.” *Hayden*, 608 F.2d at 1389 (emphasis added). (Pl. Reply at 2-3.) Pointing to a recent decision from another jurisdiction that held the TSP to be illegal and unconstitutional, see *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006),⁶⁷ plaintiff argues that the TSP is unlawful, and that Exemption 3 cannot prevent the disclosure of information relating to it because FOIA “cannot and should not be used as a method of shielding illegal governmental activity.” (Pl. Reply at 4.) Plaintiff also quotes *Terkel v. AT&T*, 441 F. Supp. 2d 899 (N.D. Ill. 2006),⁷² in which the court expressed concern, without deciding the issue, that

if, as the court in *Hayden* anticipated, section 6 is taken to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA’s functions.

Id. at 905.

While the Court agrees that the scope of Section 6 is not without limits, it need not

⁶⁷This ruling has been stayed pending appeal to the Sixth Circuit Court of Appeals. *ACLU v. NSA*, Nos. 06-2095, 06-2140, 2006 WL 2827166 (6th Cir. Oct. 4, 2006).

⁷²*Terkel* involved a suit against a telephone company arising from its alleged cooperation with the NSA to conduct surveillance under the TSP. The government intervened, and asserted, *inter alia*, the state secrets privilege and Section 6 to protect disclosure of information relating to the TSP. See *Terkel*, 441 F. Supp. 2d at 904-08.

grapple with the problem of defining those limits here, for the well-established operation of Section 6, which forbids disclosure of information relating to the NSA's SIGINT activities, is not implicated by the ongoing debate regarding the legality of the TSP. See *Linder*, 94 F.3d at 696 (holding that "[t]here can be no doubt that the disclosure of SIGINT [material] would reveal information concerning the activities of the agency," and that such disclosure was thus precluded by Section 6) (citing *Hayden*, 608 F.2d at 1389). Whether the TSP, one of the NSA's many SIGINT programs involving the collection of electronic communications, is ultimately determined to be unlawful, its potential illegality cannot be used in this case to evade the "unequivocal[]" language of Section 6, which "prohibit[s] the disclosure of information relating the NSA's functions and activities" *Linder*, 94 F.3d at 696.

The Court therefore holds that defendant's declarations describe the information withheld and "the justifications for nondisclosure with reasonably specific detail" and "demonstrate that the information withheld logically falls within" the statutory exemption of Section 6.⁸⁷ *Military Audit Project*, 656 F.2d at 738. Accordingly, as the record contains no contrary evidence or evidence of bad faith on the part of the agency, summary judgment in favor of defendant is

⁸⁷Because the Court holds that defendant properly withheld all of the requested information under Section 6, it need not reach the parties' arguments regarding 50 U.S.C. § 403-1(i)(1) and 18 U.S.C. § 798. These statutes essentially protect from disclosure information relating to the "sources," "methods," and "procedures" of the NSA's intelligence activities. Plaintiff argues that, at least with respect to requests 2-4 and 16, the information it requests does not fall within these statutory exemptions because it does not relate to NSA sources, methods, or procedures. (See Pl. Mot. at 14, 15, 17.) However, the Court is persuaded by defendant's commonsense position that the targets of the TSP are "sources" of intelligence and the TSP is a "method" of intelligence gathering. (Def. Reply at 4 n.3.) It would therefore appear that information regarding particular potential targets (request 16) and statistics regarding the number of TSP targets and the frequency of TSP surveillance (requests 2-4) are also protected from disclosure by the plain language of 50 U.S.C. § 403-1(i)(1) and 18 U.S.C. § 798.

appropriate with respect to plaintiff's five outstanding requests under FOIA Exemption 3. *See id.*

III. Exemption 1

As an alternative and independent basis for its decision, the Court holds that summary judgment is also warranted on all five of plaintiff's requests under Exemption 1, FOIA's national security exemption. Exemption 1 protects from disclosure under FOIA matters that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). Here, defendant relies on Executive Order 12958, as amended by Executive Order 13292, 68 Fed. Reg. 15315 (Mar. 25, 2003), which sets forth the standards for national security classification and specifies several categories of information which may be considered for classification. Specifically, Executive Order 12958 authorizes classification of materials relating to "intelligence activities (including special activities), intelligence sources or methods, or cryptology"^{9/} and "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection systems relating to national security" when an appropriate classification authority "determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security" Executive Order 12958 §§ 1.4(c), 1.4(g), 1.1(a)(4). To justify summary judgment under Exemption 1, an agency "must provide 'detailed and specific' information demonstrating both why the material has been kept secret and why such secrecy is allowed by the terms of [the]

^{9/}As noted above, all of the information requested by plaintiff at the very least involves NSA's "intelligence activities."

executive order.” *ACLU v. U.S. Dep’t of Justice*, 265 F. Supp. 2d 20, 27 (D.D.C. 2003) (quoting *Campbell v. U.S. Dep’t of Justice*, 164 F.3d 20, 30 (D.C. Cir. 1998)).

To that end, NSA declarant Joseph B., an original classification authority and “one of the few Agency officials who has been cleared to have access to the details of the TSP and the documents related thereto,” states that the documents responsive to requests 2-4 and 6 have been properly classified under Executive Order 12958, as their unauthorized disclosure “reasonably could be expected to cause exceptionally grave damage to the national security.” Executive Order 12958 § 1.2(a)(1). (Joseph B. Decl. ¶¶ 1, 2, 12, 19.) Specifically, he explains, the release of the statistics requested by plaintiff would reveal “information about the U.S. intelligence community’s capabilities, priorities, and activities,” and such information “about the nature and frequency of the Government’s use of specific techniques . . . could be exploited by our adversaries in order to conduct their international terrorist activities more securely, to the detriment of the national security.” (*Id.* ¶¶ 12-14.) Documents responsive to request 6, he avers, likewise “reveal details about the operation of the TSP, and its strengths and vulnerabilities, which could . . . compromis[e] the effectiveness of the program and undermin[e] its goal of detecting and preventing the next terrorist attack on the United States.” (*Id.* ¶ 19). Finally, the Joseph B. Declaration states that the fact of the existence or nonexistence of information responsive to request 16 is also properly classified under Executive Order 12958. (*Id.* ¶ 28.) As discussed above, he explains that the NSA cannot confirm or deny in any particular case whether communications were collected because over time, the accumulation of inferences from the NSA’s responses to such requests “would disclose the targets and capabilities . . . of the TSP and inform our adversaries of the degree to which NSA is aware of some of their operatives or can

successfully exploit particular communications.” (*Id.* ¶ 27.) This “compilation of information” could reasonably be expected to “cause exceptionally grave and irreparable damage to the national security” if disclosed. (*Id.* ¶ 28.)

In response, plaintiff challenges the sufficiency of the NSA’s explanations and the propriety of the classification of the withheld material in light of the “exceptional public interest” in the “general scope of the NSA’s domestic surveillance program.” (Pl. Mot. at 11-13.) Plaintiff argues that the release of only “bare statistics” and the information relating solely to whether it has been the target of surveillance could not reasonably be expected to result in the damage to the national security that defendant proclaims. (*Id.* at 11, 30.) Plaintiff also cites to section 3.1(b) of Executive Order 12958, which provides that “[i]n some exceptional cases, . . . the need to protect [sensitive] information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified” by the agency, and argues that because the public interest in disclosure here is “exceptional” and the risk to national security low, disclosure should be compelled under FOIA. (*Id.* at 12-13.) Essentially, plaintiff asks the Court to balance the potential harm of the disclosure against the public’s interest in the information. Plaintiff, however, misconstrues the statutes and well-established case law. Under Exemption 1 and the plain language of Executive Order 12958, that balancing does not rest with the Court but belongs exclusively to the agency. *See* Executive Order 12958 § 3.1(b) (The “agency head or the senior agency official . . . will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure.” (emphasis added)). Courts have repeatedly emphasized that “weigh[ing] the variety of subtle and complex factors in determining whether

the disclosure of information may lead to an unacceptable risk of compromising the intelligence-gathering process” is appropriately left to the agencies. *Ctr. for Nat'l Sec. Studies*, 331 F.3d at 927 (quoting *Sims*, 471 U.S. at 180). The Court’s role with regard to Exemption 1 is only to review the sufficiency and reasonableness of the agency’s explanation for its classification decision, giving the agency’s determination the heightened deference it is due under the law. *See Gardels*, 689 F.2d at 1104; *see also ACLU*, 265 F. Supp. 2d at 31 (“That the public has a significant and entirely legitimate desire for th[e] information simply does not, in an Exemption 1 case, alter the analysis.”).

Plaintiff also cites to section 1.7 of Executive Order 12958, which states that “[i]n no case shall information be classified in order to . . . conceal violations of law,” and again argues that because a court has recently held the TSP to be unlawful, information relating to the TSP is improperly classified. (Pl. Reply at 5.) The Court rejects this argument for substantially the same reasons explained above. Even if the TSP were ultimately determined to be illegal, it does not follow that the NSA’s decision regarding the classification of materials relating to the TSP was made “in order to . . . conceal violations of law.” Because of the deference due to the NSA in matters of national security, and in the absence of any evidence to the contrary, the Court must accept defendant’s reasonable explanation that the materials were classified in order to prevent damage to the national security. *See Gardels*, 689 F.2d at 1104.

As noted above, courts must afford agency declarations like those filed here “substantial weight” because “the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse affects [sic] might occur as a result of public disclosures of a particular classified record.” *Krikorian v. Dep’t of State*, 984 F.2d 461, 464

(D.C. Cir. 1993) (quoting *Military Audit Project*, 656 F.2d at 738); *Salisbury v. United States*, 690 F.2d 966, 970 (D.C. Cir. 1982). If the agency's declarations "are neither contradicted by other record evidence nor contaminated by indications of bad faith, the reviewing court should not ordinarily second-guess the agency's judgment." *ACLU*, 265 F. Supp. 2d at 27, 29 (noting that the agency's burden under Exemption 1 is "not especially onerous"). Having reviewed the declarations submitted by the NSA, the Court concludes that they describe "the context and nature of the withheld information," *Campbell*, 164 F.3d at 31, and the "justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith."^{10/} *Military Audit Project*, 656 F.2d at 738 (citations omitted). Because the Court is "satisfied that proper procedures have been followed and that the information logically falls into [Exemption 1], [it] need not go further to test the expertise of the agency, or to question its veracity when nothing appears to raise the issue of good faith." *Gardels*, 689 F.2d at 1104.

In short, plaintiff's arguments in favor of disclosure fall far short of overcoming the NSA's expert judgment that the disputed information must be withheld pursuant to Executive Order 12958 because it is reasonably connected to the protection of national security. *See*

^{10/}Indeed, as the parties acknowledge, this Court has previously recognized that an agency may properly invoke Exemption 1 to withhold aggregate statistical data regarding the total number of times particular surveillance tools were used. *ACLU*, 265 F. Supp. 2d at 31 (noting that "records that indicate how [an agency] has apportioned its . . . resources, that reveal the relative frequency with which particular surveillance tools are deployed, and that show how often U.S. persons have been targeted may undoubtedly prove useful to those who are the actual or potential target of such surveillance, and may thereby undermine the efficiency and effectiveness of such surveillance").

JONAS D. KRON, ATTORNEY AT LAW

P.O. Box 42093
PORTLAND, OREGON 97242
(971) 222-3366
JDKRON@KRONLAW.NET

RECEIVED
2007 JAN 10 PM 4:28
OFFICE OF CHIEF COUNSEL
CORPORATE FINANCE

January 9, 2007

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Shareholder Proposal Submitted to AT&T Inc. for 2007 Proxy Statement

Dear Sir/Madam:

I have been asked by As You Sow Foundation, Jeremy Kagan, Jeffery Hersh, Calvert Asset Management Company, Inc., Larry Fahn, The Adrian Dominican Sisters, and Cecilia Madden Charitable Trust (hereinafter referred to as "Proponents"), whom are beneficial owners of shares of common stock of AT&T Inc. (hereinafter referred to as "AT&T" or the "Company"), and who have jointly submitted a shareholder proposal (hereinafter referred to as "Proposal") to AT&T, to respond to the letter dated December 11, 2006 sent to the Office of Chief Counsel by the Company, in which AT&T contends that the Proposal may be excluded from the Company's 2007 proxy statement by virtue of Rules 14a-8(i)(2), 14a-8(i)(3), 14a-8(i)(6) and 14a-8(i)(7).

I have reviewed the Proponents' shareholder proposal, as well as the Company's letter and supporting materials, and based upon the foregoing, as well as upon a review of Rule 14a-8, it is my opinion that the Proponents' shareholder proposal must be included in AT&T's 2007 proxy statement, since (1) the Proposal, if implemented, would not cause the Company to violate the law; (2) it transcends the ordinary business of the Company by focusing on a significant social policy issue, (3) will have no substantive affect on any pending or contemplated litigation, and (4) contrary to the Company's argument, is in no way vague or indefinite. Therefore, it is respectfully requested that the Staff not issue the no-action letter sought by the Company.

Pursuant to Rule 14a-8(k), enclosed are six copies of this letter and exhibits. A copy of these materials is being mailed concurrently to AT&T Inc. Assistant General Counsel Wayne A Wirtz.

Summary Response

Based upon a review of the actual text of the Proposal and the conclusions of the Hon. Judge Vaughn R. Walker, of the U.S. District Court for the Northern District of California, in *Hepting v. AT&T* it is evident that the Proposal, if implemented, would not cause the Company to violate the law. Furthermore, the widespread concern over the allegations that AT&T is participating in the

Government's surveillance the Terrorist Surveillance Program and the Calling Records Program (the "Programs") and the resulting lawsuits demonstrate that the issues raised in the Proposal are significant social policy issues that transcend the ordinary business of the Company. Finally, the Proposal has been drafted with respect for the needs of confidentiality and in light of the disclosures about the Programs that have been made by the Government. Consequently, the Proposal is not impossible to implement. In contrast, the Proposal raises legitimate shareholder concerns about the Company's role in protecting individual rights to privacy in a balanced and reasonable fashion.

The Proposal

RESOLVED: That shareholders request that the Board of Directors issue a report to shareholders in six months, at reasonable cost and excluding confidential and proprietary information, which describes the following:

- The overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies;
- Any additional policies, procedures or technologies AT&T could implement to further ensure (a) the integrity of customers' privacy rights and the confidentiality of customer information, and (b) that customer information is only released when required by law; and
- AT&T's past expenditures on attorney's fees, experts fees, operations, lobbying and public relations/media expenses, relating to this alleged program.

Background

In December 2005, media reports alleged that President George W. Bush issued an executive order in 2001 (and repeatedly thereafter) that authorized the National Security Agency (NSA) to conduct surveillance of certain telephone calls of individuals in the United States without obtaining a warrant from a "FISA court" either before or after the surveillance. The existence of this program was confirmed by President Bush soon after it was described in the press.

In May, 2006, it was reported in the press that AT&T had provided the NSA and/or other government agencies direct access to its telecommunications facilities and databases, thereby disclosing to the government the contents of its customers' communications as well as detailed communications records about millions of its American customers.

Public knowledge of these two Programs immediately resulted in a major national controversy directly involving AT&T over significant social policy issues including the right to privacy and the legality of warrantless and/or mass electronic surveillance of American citizens. (See below for documentation of the widespread nature of the controversy).

It also resulted in more than two-dozen lawsuits seeking damages that could run to billions of dollars. AT&T is a defendant in at least 9 of these suits and in our opinion the cases represent a significant financial risk to the Company.

Due to considerable, and justifiable, concern about the significant social policy and financial implications of the Programs, this group of shareholders has decided to file a shareholder resolution with the Company. This Proposal seeks to focus the attention of management on the implications of the Programs on American citizens and the long-term wellbeing of the Company.

Furthermore, the goal of this Proposal is, as is the purpose of Rule 14a-8,¹ to facilitate a discussion between shareholders and management; and amongst shareholders about the significant policy issues facing the Company related to privacy concerns. When a company is faced with questions of such importance, shareholders have a right to communicate with management and other shareholders through the proxy statement. This group of shareholders is exercising that right through this Proposal.

What the Proposal emphatically does not do is attempt to illicit information from the Company that will compromise national security or law enforcement. Rather it seeks a report from the Company that can serve as basis for discussions about the role the Company will take, in broad general policy terms, in its pivotal position of control over customer communication data and content.

ANALYSIS

I. The Proposal, if Implemented, Would Not Cause the Company to Violate Federal Law

II. The Proposal is Focused on a Significant Policy Issue that Transcends the Ordinary Business of the Company and Therefore must be Included in the Company's Proxy.

A. The Proposal Focuses on a Significant Social Policy Issue.

B. The Proposal Does Not Focus on the Ordinary Business of the Company.

1. Litigation: The Proposal does not implicate the ordinary business litigation exclusion because it does not seek to dictate the results of any litigation.

2. Customer Privacy: It is permissible for the Proposal to focus on the freedom of expression and privacy.

¹ The purpose of Rule 14a-8 "is to provide and regulate a channel of communication among shareholders and public companies." Exchange Act Release No. 34-40018 (May 21, 1998). "The SEC continues to implement Congress's goals by providing shareholders with the right to communicate with other shareholders and with management through the dissemination of proxy material on matters of broad social import such as plant closings, tobacco production, cigarette advertising and executive compensation." *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877 (S.D.N.Y. 1993). "In so far as the shareholder has contributed an asset of value to the corporate venture, in so far as he has handed over his goods and property and money for use and increase, he has not only the clear right, but more to the point, perhaps, he has the stringent duty to exercise control over that asset for which he must keep care, guard, guide, and in general be held seriously responsible. As much as one may surrender the immediate disposition of (his) goods, he can never shirk a supervisory and secondary duty (not just a right) to make sure these goods are used justly, morally and beneficially." *Medical Committee for Human Rights v. SEC*, 432 F. 2d. 659, 680-681 (1970), vacated and dismissed as moot, 404 U.S. 402 (1972).

3. Legal Compliance: the Proposal appropriately requests that the Company consider additional policies within the Company's existing compliance structure.
4. Micro-management: the Proposal is permissible because it strikes the appropriate balance between an overly specific and excessively general request.
5. Political process: the Proposal is proper because it does not seek an evaluation of a specific legislative proposal.
6. "Touches" on a Significant Policy Issue: The Proposal must appear on the Company proxy because it directly and fully raises a Significant Policy Issue.

III. Vagueness: The Proposal does not violate the law and has struck the proper balance between specificity and generality, therefore the Company has the power and authority to implement it.

I. The Proposal, if Implemented, Would Not Cause the Company to Violate Federal Law

The Company argues that the Proposal, if implemented, would cause AT&T to violate a number of Federal laws and therefore is excludable pursuant to Rule 14a-8(i)(2). It is my opinion, after a review of the Company letter, the Sidley memorandum and the relevant law, that the Proposal, if implemented, would not cause the Company to violate the law. Specifically, we assert that (1) the state secrets privilege does not apply to this case; (2) the Hon. Judge Vaughn R. Walker has concluded that AT&T and the Government have for all intents and purposes admitted the existence of the Programs and the Company's involvement and (3) the Company has misread the Proposal and therefore has misapplied Rule 14a-8(i)(2). Consequently, we respectfully request that the Staff not concur with the Company and instead conclude that the Proposal is permissible under Rule 14a-8(i)(2).

The Company argues that the Proposal would cause AT&T to violate a number of Federal laws including 18 U.S.C. § 798(a). In essence, they are arguing that they cannot discuss any of these matters because of the state secrets privilege. This argument is misplaced, however, because the state secrets privilege is not the Company's to assert. The United States Supreme Court has ruled that the state secrets "privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party." *United States v. Reynolds* 345 U.S. 1, 7-8 (1953); see also *Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1998). Furthermore, the rules governing the assertion of the privilege require a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* Neither of these conditions have been met in this case² and consequently, this claim by the Company does not succeed. If such a claim is to be the basis of the exclusion, the Government, the holder of the privilege, would need to assert it.

Second, even assuming that the state secrets privilege has been properly petitioned for, it is false to argue that the Company can say no more than it can neither confirm nor deny its participation in the

² We note that the Company has included documentation related to the assertion of the privilege in *Terkel v. AT&T Inc.*, No. 06C-2837 (N.D. Ill.), but that assertion has not been made in *this* case with an analysis or declaration by the government of its application to the Proposal.

program. This issue was discussed at length by the Hon. Judge Vaughn Walker, the judge assigned by the Judicial Panel on Multidistrict Litigation to hear the consolidated lawsuits related to claims against the telecommunications companies. Specifically, the Hon. Judge Walker concluded,

AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content. As noted earlier, the government has publicly admitted the existence of a “terrorist surveillance program,” which the government insists is completely legal.

The Hon. Judge Vaughn R. Walker's July 20, 2006 Order in Hepting v. AT&T Corporation at p. 29 (emphasis added) Exhibit 1. The court goes on to state that “[c]onsidering the ubiquity of AT&T telecommunications services, it is unclear whether this program could even exist without AT&T’s acquiescence and cooperation.” *Id* at p. 30. Therefore, “AT&T’s assistance in national security surveillance is hardly the kind of “secret” that the . . . state secrets privilege were intended to protect . . .” *Id* at p. 3. Finally, the Hon. Judge Walker observed that “[w]hile this case has been pending, the government and telecommunications companies have made substantial public disclosures on the alleged NSA programs.” *Id* at p. 42. Please see pages 28 – 42 of The Hon. Judge Walker’s Order for a fuller discussion of his findings.

The Hon. Judge Walker also made the following point:

Based on these public disclosures, the court cannot conclude that the existence of a certification regarding the “communication content” program is a state secret. If the government’s public disclosures have been truthful, revealing whether AT&T has received a certification to assist in monitoring communication content should not reveal any new information that would assist a terrorist and adversely affect national security. And if the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements. In short, the government has opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communication content.

Id at pages 39 – 40.

Consequently, the issue whether or not the Company provided customer telephone records to the Government can hardly be called a state secret and at the very least the Company has not met its burden under Rule 14a-8(i)(2)³ of demonstrating that implementing the Proposal would violate the law. Rather the contrary is true. After extensive briefing and hearings on the issue, the judge overseeing the consolidated suits against AT&T has found that the Company and the Government have for all intents and purposes confirmed the existence of the Programs and AT&T’s participation.

Despite the length of the material provided by the Company on Rule 14a-8(i)(2), most of their argument is actually a generalized assertion that a violation of the law would occur. Nevertheless, the Company does make a few specific arguments, the first of which is an attack on the first bullet of the

3 In *The Quaker Oats Company* (April 6, 1999) the Staff wrote “neither counsel for you nor the proponent has opined as to any *compelling state law precedent*. In view of the *lack of any decided legal authority* we have determined not to express any view with respect to the application of rules 14a-8(i)(1) and 14a-8(i)(2) to the revised proposal.” (emphasis added).

proposal which asks for a report on the overarching technical, legal and ethical policy issues surrounding . . . (b) notifying customers whose information has been shared with such agencies. Specifically, the Company contends that:

notifying customers that their information had been shared as a part of a Program would (1) confirm the existence of one or both Programs, (2) confirm AT&T's participation in one or both Programs, and (3) apprise targets of federal intelligence activities that they were the subject of surveillance by federal national security agencies.

Sidley letter at page 6. First as explained above, the Hon. Judge Walker has concluded that "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content." *Walker Order* at page 29. Consequently, points (1) and (2) fail and cannot be the basis for excluding the proposal.

Second, *the Proposal never asks the Company to notify customers that their information had been shared as a part of a Program*. To state otherwise is disingenuous at best. What the Proposal does do is "request . . . a report . . . which describes . . . *The overarching technical, legal and ethical policy issues surrounding . . . (b) notifying customers whose information has been shared with such agencies (the FBI, NSA and other government agencies).*" This is a request for a generalized policy discussion about what could or would be involved in notifying customers whose information has been shared with the FBI, NSA or other government agencies. It also is not limited to the Programs. Undoubtedly, AT&T regularly shares customer information with the FBI and other government agencies (state or federal) in the course of routine criminal law enforcement. Consequently, a policy discussion about the Company's involvement in law enforcement is not a de facto confirmation of participation in the Programs. Furthermore, to the extent that a portion of the discussion implicates confidential (i.e. classified) matters, the Proposal provides for excluding that information.

Next the Company argues that a request "detailing the expenditures made by the Company for the 'operations' associated with these Programs would confirm their existence, confirm AT&T's participation in them, and furnish information concerning their scope." Sidley letter at page 6. Once again, this assertion does not succeed because, as the Hon. Judge Walker found, "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content." *Walker Order* at p. 29. The Government and the Company have, for all intents and purposes already confirmed their existence and confirmed AT&T's participation in them, so to now claim the Proposal is excludable because it would allegedly cause this confirmation is to deny judicially established facts.

As for the third contention regarding scope, it is worth repeating that there is nothing in this Proposal that requires them to disclose confidential information, because the Proposal specifically provides for "excluding confidential information." In this case the Company could simply do the following in a report:

AT&T's past expenditures on operations relating to the alleged Programs

Due to federal laws on classified information, the Company is unable to furnish information concerning the alleged scope of the Programs and therefore is unable to detail AT&T's past expenditures on operations relating to the alleged Programs. However, certain general

statements can be made in this regard . . .

Furthermore, this portion of the Proposal *only requires a "description" of the expenses - not an accounting*. This is not to say the Proposal is meaningless, as discussed elsewhere in this letter the Proposal covers (1) material that extends beyond the Programs, (2) allows for excluding confidential information, and, most importantly, (3) focuses on the broad social policy issues the Company faces as it addresses the privacy concerns of its customers, shareholders and policy makers.

Simply stated, in keeping with the findings and reasoning of the court, the Proposal, if implemented, does not require the disclosure of any state secrets. The Company's primary argument has been that any discussion is prohibited because the existence of the Programs and the Company's participation in the Programs is a state secret. Clearly it does not constitute a state secret and therefore cannot be the basis for exclusion.

In addition, it is evident that the Company is capable of discussing the issues raised in the Proposal in a public forum. In fact, this very proceeding before the Commission is a discussion of the legal issues surrounding AT&T's alleged cooperation with government agencies. The Sidley memo provides a perfect template for how such a discussion could take place even assuming the Company cannot confirm nor deny participation in the Programs. The fifth paragraph (pg. 2) reads as follows:

AT&T cannot confirm or deny any reports alleging participation in federal intelligence activities, including the Programs. For purposes of responding to your request only, we accept at face value the asserted facts reported in the newspapers and targeted by the Proposal. No inference can or should be drawn from these assumptions made only for the purposes of this analysis regarding the truth or falsity or [sic] any such allegations, and nothing herein should be construed as an admission or denial of any allegation relating to such Programs.

It is assumed that any report to shareholders would contain the same or similar language making clear that the Company cannot (absent permission from the government) discuss the *details* of an intelligence program or disclose its existence. However, the parameters of such a discussion – the importance of privacy versus national security and the responsible role of a corporation in weighing those two values – is clear. A report could be written that discusses these issues in the abstract without revealing classified information.⁴ There is nothing confidential about the law surrounding the sharing of telephone information.

The Company could also readily have a portion of the report be devoted to discussing the ethical issues that the Company should consider in light of the public media reports of law enforcement requests for information. This discussion could include the constitutional principles at issue, historical examples, the costs and benefits to society of different Company policies on how to respond to law enforcement

4 We note that the Company has cited *People for the American Way Foundation v. NSA et al.*, Civil Action No. 06-206 (ESH) (Nov. 20, 2006) for the proposition that basic numerical or statistical information about the Terrorist Surveillance Program is classified. That case does not apply to the Proposal for a number of reasons including, the defendant in that case was the NSA (not AT&T or another telecom company); the law at issue was FOIA (not Rule 14a8); it was a motion for summary judgment; and it only applied to one of the two Programs (the Terrorist Surveillance Program). Consequently, it does not constitute compelling or decided legal authority and cannot be a basis for exclusion. Second, the Proposal does not seek numerical or statistical information about either program and therefore the two cases are not analogous.

requests for cooperation as described in media stories, in short it can be a generalized discussion of the policy issues that the Company is facing when privacy issues are raised.

Furthermore, AT&T could discuss these issues in the *hypothetical* event that AT&T is asked in the future to disclose confidential customer information pursuant to a secret government program. Even assuming that the Company cannot describe what has *happened*, it is not prohibited from describing how the Company would or could in the *future* apply the known structures of federal law to government requests for otherwise private information.⁵

Also, we note that other telecommunications companies, specifically Qwest, BellSouth and Verizon, have all made public declarations denying any involvement in the Programs. See John O'Neil and Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained*, New York Times, May 12, 2006 (Exhibit 2) and FoxNews: *Verizon- We Didn't Give Customers' Call Records to NSA Either*, May 16, 2006 <http://www.foxnews.com/printer_friendly_story/0,3566,195745,00.html>. Exhibit 3.

As the Hon. Judge Walker observed

BellSouth, Verizon and Qwest have publicly denied participating in the alleged communication records program Importantly, the public denials by these telecommunications companies undercut the government and AT&T's contention that revealing AT&T's involvement or lack thereof in the program would disclose a state secret.

Walker Order at page 41. Given that these companies apparently do not believe there is any reason they cannot deny their involvement it is unclear why AT&T would feel compelled to make the argument in its no-action request letter other than to obfuscate the true validity of the Proposal.

Going beyond those points, however, we also maintain that the Company's claims are erroneously based on a mis-characterization of what the Proposal actually is requesting of the Company - thereby allowing them to construct a straw-man that they can knock down. The Sidley letter, in particular, has tried to respond by reading the word "confidential" out of the Proposal. In addition, the Sidley letter fails to acknowledge that the Proposal is focused on a broad set of policy issues that reach beyond the particulars of the Terrorist Surveillance Program or the Calling Records Program. A full third of the whereas clauses do not address the Programs, but rather are focused on the general, overarching issue of privacy. The following three whereas clauses are a clear demonstration of the focus on the Proposal being not limited to the Programs.

WHEREAS: The right to privacy is a long established value, enshrined in the Constitution and decades of U.S. jurisprudence, and cherished by people of all political persuasions; and

WHEREAS: Privacy protections serve many important societal purposes: encouraging development of science and knowledge; preventing fraud; and allowing individuals to communicate sensitive information (i.e. health care providers, clergy, brokers); and

WHEREAS: In light of the potentially negative uses of today's technology, we believe it is

⁵ This is also the reasoning adopted in the Vermont Public Service Board's denial of AT&T's motion to dismiss. See *Petition of Vermont Department of Public Service* Docket No. 7193, Order on Motion to Dismiss at p. 18. Exhibit 9.

important that AT&T re-examine the steps it takes to protect the values embodied in an individual's right to privacy.

Furthermore, the actual resolve clause makes only one reference to the Programs and for the overwhelming majority of its text focuses on the privacy of customer communications and records regardless of any relationship to the Programs. It almost goes without saying that AT&T is regularly asked to confront privacy issues as they relate to subjects such as criminal matters, identity theft and pretexting. This proposal clearly is concerned with the Programs, but to say that it is limited to the Programs is a disingenuous attempt to ignore half of the language in the Proposal.

As noted earlier, in *The Quaker Oats Company* (April 6, 1999) the Staff wrote "neither counsel for you nor the proponent has opined as to any **compelling** state law precedent. In view of the lack of any **decided legal authority** we have determined not to express any view with respect to the application of rules 14a-8(i)(1) and 14a-8(i)(2) to the revised proposal." (emphasis added). We observe that the Company has not cited to any example of the state secrets privilege or any other national security law being applied to shareholder proposals or other provisions of the proxy rules. Furthermore, they have not established any decided legal authority on this issue. In fact, the Hon. Judge Walker's Order indicates that the Company's assertions of the law are misplaced and that the decided legal authority runs contrary to their position. Consequently, the Company has not met its burden and we respectfully request the Staff conclude that Rule 14a-8(i)(2) does not apply to the Proposal. In the alternative, and in light of *The Quaker Oats Company*, we request that the Staff not express any view with the respect to the application of Rule 14a-8(i)(2).

In conclusion, it is abundantly clear that the Company would be able to implement the Proposal without violating the law. Whether it be the compelling conclusions of the Hon. Judge Walker or the accurate reading of the Proposal, in both cases it is apparent that the Proposal is asking the Company to discuss the privacy issues facing the Company at an appropriately general level that will not violate the law. These issues are being discussed already in public and in the courts and they rightfully should be discussed by the Company with its shareholders as well.

II. The Proposal is Focused on a Significant Policy Issue that Transcends the Ordinary Business of the Company and Therefore must be Included in the Company's Proxy.

Rule 14a-8(i)(7), the ordinary business exclusion, is based on the corporate law principle that particular decisions are best left to management because they are in a better position than shareholders to make those day-to-day decisions. *However*, when a company encounters issues of significant social policy importance, it is no longer the case that management is in a better position than shareholders to evaluate how the company should address the issue. Rather when the Company is facing a significant social policy issue, the shareholders have an appropriate and legitimate role to play. Consequently, under the ordinary business exclusion, management's role must yield to the rights of shareholders to raise, consider and opine on those matters which have significant social consequences.

A. The Proposal Focuses on a Significant Social Policy Issue.

A proposal cannot be excluded by Rule 14a-8(i)(7) if it focuses on significant policy issues. As

explained in *Roosevelt v. E.I. DuPont de Nemours & Company*, 958 F. 2d 416 (DC Cir. 1992) a proposal may not be excluded if it has "significant policy, economic or other implications". *Id.* at 426. Interpreting that standard, the court spoke of actions which are "extraordinary, i.e., one involving 'fundamental business strategy' or 'long term goals.'" *Id.* at 427.

Earlier courts have pointed out that the overriding purpose of Section 14a-8 "is to assure to corporate shareholders the ability to exercise their right – some would say their duty – to control the important decisions which affect them in their capacity as stockholders." *Medical Committee for Human Rights v. SEC*, 432 F. 2d. 659, 680-681 (1970), vacated and dismissed as moot, 404 U.S. 402 (1972).

Accordingly, for decades, the SEC has held that "where proposals involve business matters that are mundane in nature and ***do not involve any substantial policy or other considerations***, the subparagraph may be relied upon to omit them." *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877, 891 (S.D.N.Y. 1993) quoting Exchange Act Release No. 12999, 41 Fed. Reg. 52,994, 52,998 (Dec. 3, 1976) ("1976 Interpretive Release") (emphasis added).

It has been also been pointed out that the 1976 Interpretive Release explicitly recognizes "that all proposals could be seen as involving some aspect of day-to-day business operations. That recognition underlays the Release's statement that the SEC's determination of whether a company may exclude a proposal should not depend on whether the proposal could be characterized as involving some day-to-day business matter. Rather, ***the proposal may be excluded only after the proposal is also found to raise no substantial policy consideration.***" *Id.*

Most recently, the SEC clarified in Exchange Act Release No. 34-40018 (May 21, 1998) ("1998 Interpretive Release") that "Ordinary Business" determinations would hinge on two factors.

Subject Matter of the Proposal: "Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as hiring, promotion, and termination of employees, decisions on the production quality and quantity, and the retention of suppliers. However, ***proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable***, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote." 1998 Interpretive Release (emphasis added)

"Micro-Managing" the Company: The Commission indicated that shareholders, as a group, will not be in a position to make an informed judgment if the "proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Such micro-management may occur where the proposal "seeks intricate detail, or seeks specific time-frames or methods for implementing complex policies." However, "timing questions, for instance, could involve significant policy where large differences are at stake, and proposals may seek a reasonable level of detail without running afoul of these considerations."

It is vitally important to observe that the company bears the burden of persuasion on this question. Rule 14a-8(g). The SEC has made it clear that under the Rule "***the burden is on the company to***

demonstrate that it is entitled to exclude a proposal.” Id. (emphasis added).

We also note that recently the Second Circuit has ruled on a Rule 14a-8 matter in *AFSCME v. AIG*. One of the principles supporting that decision is the following:

Although the SEC has substantial discretion to adopt new interpretations of its own regulations in light of, for example, changes in the capital markets or even simply because of a shift in the Commission’s regulatory approach, it nevertheless has a “duty to explain its departure from prior norms.” *Atchison, T. & S. F. Ry. Co v. Wichita Bd. of Trade*, 412 U.S. 800, 808 (1973) (citing *Sec. of Agric. v. United States*, 347 U.S. 645, 652-53 (1954)); cf. *Torrington Extend-A-Care Employee Ass’n v. NLRB*, 17 F.3d 580, 589 (2d Cir. 1994) (stating that “an agency may alter its interpretation of a statute so long as the new rule is consistent with the statute, applies to all litigants, and is supported by a ‘reasoned analysis’”). *Id.*

Therefore it is apparent that the Second Circuit, noting the lack of “reasoned analysis”, has reaffirmed the importance of the SEC staff adhering to the 1976 and 1998 Interpretive Releases.

Consequently, when analyzing this case, it is incumbent on the Company to demonstrate that the Proposal does not involve any substantial policy or other considerations. Therefore, it is only when the Company is able to show that the Proposal raises *no* substantial policy consideration that it may exclude the Proposal. Clearly, this is a very high threshold that gives the benefit of the doubt to the Proponents and tends towards allowing, rather than excluding, the Proposal.

Examples of how significant of a social policy issue consumers’ telephone and communications privacy has become are abundant:

- A May 2006 Gallup Poll found that 67% of Americans say that they are very closely or somewhat closely following reports that “a federal government agency obtained records from three of the largest U.S. telephone companies in order to create a database of billions of telephone numbers dialed by Americans” <http://www.galluppoll.com/content/default.aspx?ci=5263>. Exhibit 4. This is consistent with a December 2005 poll by the Rasmussen Report which concluded that “Sixty-eight percent (68%) of Americans say they are following the NSA story somewhat or very closely.” <http://www.rasmussenreports.com/2005/NSA.htm>. Exhibit 5. This clearly demonstrates that the issue has persistent and widespread interest in American society.
- The issue has resulted in numerous reports by print, radio, television and Internet media. Attached in Exhibit 6 is a partial list of more than 40 stories on the issue from media outlets including the New York Times, USA Today, Wired Magazine, CBS, CNN and National Public Radio.
- The issue has been the subject of substantial interest by politicians and regulators. During the 109th Congress, the Senate Judiciary Committee subpoenaed the heads of several telecommunications companies to testify about the program and it was only at the behest of the Vice President of the United States that hearings on this issue were temporarily halted. John Diamond, *Specter: Cheney put pressure on panel*, USA Today, June 7, 2006; John Diamond, *Senators won’t grill phone companies*, USA Today, June 7, 2006.

- Senator Patrick Leahy, (D-VT), the incoming chairman of the Senate Judiciary Committee, has expressed concern about the need for the companies allegedly involved to be held accountable if wrongdoing is found. "These companies may have violated the privacy rights of millions of Americans," Leahy said. "Immunity as a general rule in any industry can be a dangerous proposition for it promotes less accountability." Rebecca Carr, *Bush is seeking immunity for telecom industry*, Cox News, November 15, 2006.
- Several key national politicians and regulators have called for investigation into the scandal including Federal Communications Commissioner Michael Copps (Exhibit 7) and Representative Edward Markey (D- MA) (Exhibit 8), the then ranking minority member of the House Subcommittee on Telecommunications and the Internet.
- State utility regulators have also devoted substantial time and attention to the issue. Investigations of the telecommunications companies phone record sharing have been instituted in Vermont, Maine, New Jersey, Connecticut, and Missouri. Exhibit 9. Hearings on the issue have been held in a number of other states including Washington, Delaware, Nebraska, and Pennsylvania. Exhibit 10.
- Local officials have also expressed concerns. San Francisco Mayor Gavin Newsom has indicated that he will perform a full review of all of AT&T's contracts with the city in light of their alleged participation in this scandal. Scott Lindlaw, *SF Reviews Contracts with AT&T Over Domestic Spying*, Associated Press, July 11, 2006. <http://sfgate.com/cgi-bin/article.cgi?f=/news/archive/2006/07/11/financial/f140225D55.DTL> Exhibit 11.
- The possibility that AT&T has shared phone records has also exposed the company to substantial potential liability. More than two-dozen lawsuits have been filed seeking damages that could run to billions of dollars. Ryan Singel, *AT&T Sued Over NSA Eavesdropping*, Wired, January 31, 2006. (<http://www.wired.com/news/technology/0,70126-0.html> Exhibit 12. AT&T is a defendant in at least 9 of these suits and in our opinion the cases represent a significant financial risk to the Company.
- A May 2006 Newsweek Poll indicated that "53 percent of Americans think the NSA's surveillance program 'goes too far in invading people's privacy,'" The report on the poll specifically discussed the allegation that the "NSA has collected tens of millions of customer phone records from AT&T Inc." <http://www.msnbc.msn.com/id/12771821> Exhibit 13.
- At Cisco Systems, Inc.'s November 2006 Annual Meeting, a shareholder proposal asking the company to address "steps the company could reasonably take to reduce the likelihood that its business practices might enable or encourage the violation of human rights, including freedom of expression and privacy . . ." received a noteworthy **29% of the vote**. <http://www.bostoncommonasset.com/news/cisco-agm-111506.html> Exhibit 14. This vote is a clear expression of considerable shareholder concern about the role that technology and communications companies play in the freedom of expression and privacy.

In short, it is evident that the issue has become significant in a wide spectrum of venues including polling, media, congressional leadership and hearings, federal and state administrative investigations,

locally and in the courts.

It is also evident that the issue of telecommunications privacy has already been well established as a significant social policy issue. See, *Cisco Systems Inc.* (July 13, 2002). In *Cisco*, the proposal focused on the freedom of expression, association and privacy – specifically requesting that Cisco report to shareholders on the capabilities of its hardware and software products that allow monitoring and/or recording of Internet traffic. The company attacked the proposal on various grounds including that it did not focus on a significant policy issue. That argument was rejected by the SEC staff in its conclusion that these issues were in fact significant policy issues. It is also interesting to note the following statements made by Cisco in its ordinary business argument:

The capabilities which Proponent is addressing meet fundamental and legitimate needs to protect the integrity of Internet communications networks against theft, sabotage, viruses, unlawful intrusion and other unlawful activities. For example, Cisco products used by its customers, whether a private business, a telecommunications service provider or the Securities and Exchange Commission, have these capabilities, as do the products of its competitors. Proponent argues that the use of these capabilities by governments for monitoring is a threat to freedom of speech for all world-wide users. However, such capabilities are legitimately used by governments for the foregoing purposes and are also used by the United States and other countries for law enforcement and national security purposes and to protect their citizens against the threat of terrorism. *Of course, in the United States and other countries whose systems are based upon the rule of law, the exercise of these powers is subject to constitutional and legal protections and respect for individual rights.* The report required by the Second Proposal would address none of *these significant social policy issues.* (emphasis added)

We believe that Cisco had it right when it stated that the the balance between national security/law enforcement and the constitutional and legal protections for individual rights is a significant social policy issue that is properly addressed in a shareholder proposal like the one submitted by the Proponents.

The issues raised by the alleged participation of AT&T in the Programs and the resulting controversy and financial risks transcend the day-to-day affairs of the Company. These are issues that shareholders are appropriately concerned about and as a result we have the right to raise these issues at AT&T's annual meeting and express our opinion about how the Company should explore its role in protecting the privacy of American citizens. These issues are beyond a doubt significant social policy issues that have captured the attention of millions of Americans; federal, state and local politicians; and are clearly of concern to other investors. We respectfully believe the Staff should reach the same conclusion and notify the Company that it cannot exclude the Proposal as merely focusing on the day-to-day business of AT&T.

B. The Proposal Does Not Focus on the Ordinary Business of the Company.

As discussed at length above, all shareholder proposals can be seen as involving some aspect of a company's day-to-day business operations. So while it is important to consider the issues raised by the Company, ultimately, “the proposal may be excluded only after the proposal is also found to raise no

substantial policy consideration.”

1. Litigation: The Proposal does not implicate the ordinary business litigation exclusion because it does not seek to dictate the results of any litigation.

The Company also asserts that the Proposal is excludible as affecting its litigation strategy and the discovery process of numerous proceedings. First, it should be noted once again that the Proposal allows the Company to exclude "confidential information," which includes matters of litigation strategy and discovery related issues. Nowhere does the Proposal, expressly or implicitly, require a report on how the Company plans to argue the procedural or substantive aspects of any legal case or how it expects to resolve the cases. Instead what is contemplated by the Proponents is reporting on the overarching policy issues, descriptions of alternative future policies, and general descriptions of past expenditures. Finally, we note that the Company does very little to flesh out its general assertions that the Proposal interferes with litigation and essentially does little more than make the bald assertion and cite cases that support the general rule without making an effort to analogize those cases to the Proposal.

Reynolds American Inc. (February 10, 2006). In that case, the proposal requested the company “undertake a campaign aimed at African Americans apprising them of the unique health hazards to them associated with smoking menthol cigarettes” while at the same time the company was a defendant in a lawsuit in which the Company was disputing “ the use of menthol cigarettes by the African American community poses unique health risks to this community.” In other words, if the proposal was enacted, the Company would have directly conceded the central point of the litigation and essentially mooted the litigation. Examining the Proposal in light of this case, an analogy would exist only if the Proposal sought the Company make some sort of statement that it has (as it characterizes the lawsuits) “violated consumer privacy rights”. This is not what the Proposal does. Our Proposal requests an overarching policy discussion of the issues surrounding privacy rights and does not request the Company come to any particular conclusion regarding those rights and does not seek thereby to dictate the results of the lawsuits. Consequently, *Reynolds* cannot provide a basis for exclusion.

R.J. Reynolds Tobacco Holdings, Inc. (February 6, 2004). In this example, the proposal asked:

RJR stop all advertising, marketing and sale of cigarettes using the terms "light," "ultralight," "mild" and similar words and/or colors and images until shareholders can be assured through independent research that light and ultralight brands actually do reduce the risk of smoking-related diseases, including cancer and heart disease

At the same time the Company was arguing that it was entitled to advertise and market cigarettes using the terms "light," "ultralight," "mild" and similar words. That is, if the proposal had passed the result would have been to moot the litigation because the litigation would have been resolved. Consequently, it is evident that *R.J. Reynolds Tobacco Holdings, Inc.* (February 6, 2004) is not dispositive in this case because there is nothing in our Proposal that would resolve the litigation that the Company refers to. For the Company argument to be valid, the Proposal would need to some how result in the litigation being resolved. Clearly a request for an overarching policy discussion of privacy issues as they relate to cooperating with local, state and federal authorities and a request for a description (not an accounting) of past expenses does not directly or indirectly dispose of any litigation the Company is engaged in.

R.J. Reynolds Tobacco Holdings, Inc. (March 6, 2003). Here, the resolution was designed to resolve the pending litigation against the company regarding its smuggling practices. In particular, the resolution required the company to “determine the extent of our Company’s past or present involvement directly or indirectly in any smuggling of its cigarettes throughout the world.” The litigation pending against the company was seeking precisely these outcomes. So implementation of the resolution could have effectively meant resolving the litigation. In other words, this resolution fit into the ordinary business precedents “when the subject matter of the proposal is the same or similar to that which is at the heart of litigation in which a registrant is then involved.” That is far from the situation in our resolution. The Proposal does not request, directly or even indirectly, any assessment about the litigation nor require any outcome to the litigation.

Similar conclusions must also be reached upon thorough review and analysis of the five other cases cited by the Company on the bottom of page five of its letter. As the Company made very clear in its brief descriptions of the cases, they were all examples of proposals requesting certain actions to be taken by the company that were expressly and directly linked to specific actions in specific pending or contemplated litigation. *NetCurrent, Inc.* (May 8, 2001) (requiring the company **to bring an action in court**); *Microsoft Corporation* (September 15, 2000) (asking the company **to sue the federal government**); *Exxon Mobil Corporation* (March 21, 2000) (requesting the company **to make settlement payments**); *Philip Morris Companies* (February 4, 1997) (recommending the company **to implement regulations that it was challenging in court**); and *Exxon Corporation* (December 20, 1995) (asking the company **to forgo appellate rights**).

The Proposal does not expressly, let alone impliedly, request the Company to bring an action in court, to sue anyone, to make settlement payments, to implement regulations, forgo appellate rights or do anything that could be said to involve whether or how the Company will litigate the cases.

In essence the Company is arguing that if there is a lawsuit on the matter then the Company is per se allowed to exclude any shareholder proposals on the matter. Clearly that is not the case. Consider for example the following examples which are more analogous to the Proposal:

In *RJ Reynolds* (March 7, 2000) the company had to include a resolution that called for the company to create an independent committee to investigate retail placement of tobacco products, in an effort to prevent theft by minors. The company argued that due to two current lawsuits (against FDA and the state of Massachusetts) the Proposal, if implemented, would interfere with litigation strategy by asking the company to take voluntary action in opposition to its position in the lawsuits. The proponent prevailed by arguing that it addressed a significant policy issue (tobacco and children) and that the Proposal is unrelated to litigation. “[L]itigation strategy has been interpreted to encompass matters ranging from the decision whether to institute legal proceedings, to the conduct of a lawsuit, to the decision whether to settle a claim or appeal a judgment.” That proposal, as the present one now being considered, deals with none of the above.

In *Philip Morris* (February 14, 2000), the proposal called for management to develop a report for shareholders describing how Philip Morris intends to address “sicknesses” caused by the company’s products and correct the defects in the products that cause these sicknesses. The company argued that the proposal requested the company to issue a report on matters that are prominently at issue in numerous lawsuits. The proponent prevailed by arguing that the proposal neither requests information about litigation nor tells the company how to handle the litigation. Due to statements on the company’s web site, essentially admitting to cigarettes causing “sickness,” the proposal asking how the company will address that “sickness” would not likely interfere with any litigation strategy. Similarly, because the Company has already engaged

in some general discussions of the Programs, our Proposal will not interfere with any litigation strategy.

In *Bristol-Myers Squibb Company* (February 21, 2000), the resolution called for implementation of a policy of price restraint on pharmaceutical products for individual customers and institutional purchasers to keep drug prices at reasonable levels and report to shareholders on any changes in its current pricing policy by September 2000. The company argued that the Proposal sought to have the company take action in an area of its business currently subject to litigation: its pricing practices. The proponent prevailed -- arguing that as a matter of good public policy a proposal raising a broad policy issue should not be automatically excluded if the company has at sometime, somewhere, been sued in connection with a related matter. Our Proposal is analogous to this case because it raises a broad policy issue that happens to be implicated in a number of settings, including litigation.

Further, the mere mention of lawsuit in a shareholder resolution does not render the resolution excludible as ordinary business. In *RJR Nabisco* (February 13, 1998), the resolution called for the company to implement in developing countries the same programs for prevention of smoking by youths as voluntarily proposed and adopted in US. The company mentioned that proponents refer to lawsuits against subsidiaries in France and Philippines dealing with alleged violations of marketing regulations as a basis for extending the US policy abroad. The proponent prevailed by pointing out that the company has already implemented these programs in the US and therefore has nothing to do with lobbying/litigation strategies.

In sum, this analysis demonstrates that the Proposal does not interfere with any litigation the Company is, or may be, engaged in. It does not direct any particular result nor does it require the Company to divulge its strategies. Rather it is properly focused on the broad yet very significant social policy issues confronting the Company at this time.

2. Customer Privacy: It is permissible for the Proposal to focus on the freedom of expression and privacy.

The Company further argues that the Proposal should be excluded because it improperly relates to customer privacy. In support of this contention the Company cites two cases: *Bank of America Corp.* (February 21, 2006) and *Applied Digital Solutions, Inc.* (March 25, 2006).

Addressing *Applied Digital Solutions, Inc.* first, it is important to observe that the Company erroneously stated that this proposal was excluded as relating to "procedures for protecting customer information". Rather a review of the Staff letter on this proposal shows that the proposal was excluded because it related to "product development" - a very different reason. Consequently, *Applied Digital Solutions, Inc.* is not relevant to this discussion and cannot be a basis for exclusion.

With respect to *Bank of America Corp.* (February 21, 2006), that proposal stated:

Therefore, be it resolved that the Board of Directors report to shareholders no later than July 2006 on the company's policies and procedures for ensuring that all personal and private information pertaining to all Bank of America customers will remain confidential in all business operations. This report should also cover policies relating to those employees of contractors and subcontractors hired by the company.

Contrary to the assertion of the Company, that proposal is quite distinct from our Proposal. *Bank of America Corp.* simply requested a mere cataloging of existing policies and procedures for ensuring confidentiality not unlike the “general conduct of a legal compliance program” exclusion discussed below in subsection 3. The Proposal, in contrast, goes far beyond a day-to-day issue in that it requests a description of overarching policy issues, past expenditures and **additional policies**. Our Proposal does not simply focus on a mundane matter like describing existing policies or mere procedural issues, but rather focuses on the significant policy issues of the societal and business concerns facing the Company as the result of the allegations relating to the Programs.⁶

Instead of looking to *Bank of America*, it is more instructive to review the Proposal in light of *Cisco Systems Inc.* (July 13, 2002) cited earlier. In *Cisco*, the proposal focused on the freedom of expression, association and privacy – specifically requesting a report:

which describes the capabilities of Cisco hardware and software that is sold, leased, licensed, or otherwise provided to any government agency or state-owned communications/information technology entity(ies) in any country (a) which could allow monitoring, interception, keyword searches, and/or recording of internet traffic . . .

Both the Cisco proposal and the Proposal seek to address the same significant policy issue – privacy rights. Further, both proposals address issues surrounding the implications of monitoring, intercepting and recording telecommunications data and content; and the use of that information by the government. In these ways, the Proposal is completely analogous to *Cisco* and therefore it should be treated by the SEC as permissible.

3. Legal Compliance: the Proposal appropriately requests that the Company consider additional policies within the Company's existing compliance structure.

The Company further asserts that the Proposal is excludible because it improperly relates to legal compliance matters. This analysis is incorrect, however, because it is clear that proposals are permitted to address **additional measures** that can be analyzed and taken within the **existing legal compliance structures**. Upon further examination, it is clear that none of the cases cited by the Company apply and that there are analogous examples of permissible proposals.

In, *Allstate Corporation* (February 16, 1999) the proponents sought to create an entirely new committee that would hire experts in “the fields of: Criminal Law, Mc Carran Ferguson Act, Bad Faith Insurance Actions, Shareholders Derivative Actions and a Financial Management firm be organized for the purpose of investigating the issues raised”. This proposal is distinct in two ways from the Proposal. First, *Allstate* sought to create a whole new compliance structure for the company. The Proposal, in contrast, does not do that – it simply requests a discussion, within the existing compliance mechanisms, of potential future policies that could be implemented. Second, the *Allstate* proposal achieved a comparatively high level of micro-management that the Proposal does not. That proposal sought to dictate how the compliance program would occur with specifics about certain fields of law and the

⁶ We also observe that in *Bank of America* the proponent did not offer any discussion of analysis of Rule 14a-8(i)(7), but made a few conclusory statements in response to the no-action request. Consequently, that proposal does not represent a full consideration of the issues.

need to hire specific personnel to staff the committee. The Proposal in contrast appropriately leaves those questions, ultimately management issues, within the discretion of the Board and simply focuses on the significant social policy issues facing the Company.

Similarly, the *Monsanto Company* (November 3, 2005) proposal requested the creation of an ethics oversight committee to "insure compliance with the Monsanto Code of Conduct, the Monsanto Pledge, and applicable laws, rules and regulations of federal, state, provincial and local governments, including the Foreign Corrupt Practices Act." While falling short of the micro-managing staffing requirements, the *Monsanto* proposal is flawed in the same ways as *Allstate*. In contrast to the Proposal, *Monsanto* tried to create a separate compliance structure and mechanism and sought to dictate the precise statutes to be considered. Our Proposal is distinct from *Monsanto* in that it works within the existing compliance structures of the Company and therefore *Monsanto* cannot be grounds for exclusion.

The *Halliburton Company* (March 10, 2006) proposal, cited by the Company, requested a report "on the policies and procedures adopted and implemented to reduce or eliminate the reoccurrence of such [criminal] violations and investigations." This proposal was excluded as addressing "general conduct of a legal compliance program." What is distinct about *Halliburton* is that the proposal simply sought a mere recitation of policies – a request that can fairly be described as relating to the "general conduct of a legal compliance program." Where *Monsanto* and *Allstate* went too far, *Halliburton* was too vague and general. In contrast, our Proposal strikes the correct balance and requests the Company, within its existing mechanisms, conduct an analysis and discussion of *additional* measures that could be taken in the future. Consequently, *Halliburton* does not apply to this case.

Finally, in *Duke Power Company* (February 16, 1999) the shareholder sought what can only be described as extremely detailed information on the technical aspects of a highly regulated portion of the company's business. In fact the resolve clause ran almost 300 words and included a list of very specific technical information on particular facilities. It is erroneous to analogize our Proposal to *Duke* for the very simple reason that the *Duke* proposal achieved an extraordinary level of micro-management in a very highly regulated and technical aspect of pollution controls. The Proposal in contrast raises, at a general level, questions of *additional* policies, procedures or technologies to protect customers constitutional rights to privacy, freedom and association.

In contrast to the cases cited by the Company, consider for example the proposal in *Dow Chemical Company* (February 28, 2005) which sought an analysis of the adequacy and effectiveness of the "company's internal controls related to potential adverse impacts associated with genetically engineered organisms" which the Staff concluded was permissible. The allowed *Dow* proposal is analogous to our Proposal in two ways. First, both proposals seek a discussion about how the company is addressing a significant policy issue – adverse impacts associated with genetically engineered organisms on the one hand and privacy rights on the other. Both also seek a discussion of additional measures – improved effectiveness of the company's internal controls in one case and additional policies in the Proposal.

Also, consider *Bank of America Corp.* (February 23, 2006) in which the Staff denied a no-action request for a shareholder proposal, which requested that this company's board "develop higher standards for the securitization of subprime loans to preclude the securitization of loans involving predatory practices" (an illegal practice). The company challenged the proposal on the grounds that the proposal dealt with "a general compliance program" because it sought to ensure that the company did not engage in an illegal practice. The Staff rejected that reasoning and we respectfully submit that the

Staff should do so again. In both our Proposal and the *Bank of America Corp.* proposal, the resolutions focus on improving policies and taking further steps to ensure that the company appropriately addresses a significant policy issue within the existing compliance system. It is clear from this case that it is proper for proposals to focus on *additional steps* that a company can take to improve its policies.

In conclusion, we respectfully request the Staff conclude that the Proposal appropriately touches on improvements to the existing compliance structures and does not seek to micro-manage the Company or otherwise create new compliance mechanisms.

4. Micro-management: the Proposal is permissible because it strikes the appropriate balance between an overly specific and excessively general request.

The Company also asserts that the Proposal seeks to micro-manage the company by addressing complex matters. While the appropriateness of this Proposal for shareholder consideration is addressed throughout this letter it is important to briefly respond to the charge of micro-management. As discussed earlier, the Commission has indicated that shareholders, as a group, will not be in a position to make an informed judgment if a "proposal seeks to 'micro-manage' the company by *probing too deeply* into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Such micro-management may occur where the proposal "*seeks intricate detail*, or seeks specific time-frames or methods for implementing complex policies." However, "timing questions, for instance, could involve significant policy where large differences are at stake, and *proposals may seek a reasonable level of detail* without running afoul of these considerations." 1998 Interpretive Release.

In light of this standard, it would be false to conclude that a proposal that seeks a general report on "overarching" issues and policies is seeking "intricate detail". Furthermore, there is a long line of precedents that support a request for information on past expenditures. See *Chevron Corporation* (February 28, 2006) (seeking "annual expenditures by category for each year from 1993 to 2005, for attorneys' fees, expert fees, lobbying, and public relations/media expenses, relating in any way to the health and environmental consequences of hydrocarbon exposures and Chevron's remediation of Texaco drilling sites in Ecuador and (b) expenditures on the remediation of the Ecuador sites.); *E.I. du Pont de Nemours and Company* (February 28, 2005) (virtually identical language); and *General Electric Company* (February 2, 2004) (virtually identical language).

This Proposal in fact strikes the appropriate balance between being specific enough not to be vague or indefinite and general enough not to be micro-managing the Company. We also note that in the Company's vagueness argument that is addressed more fully below in section 3, the Company does not claim that the proposal is vague in the sense that particular words are not sufficiently specific or are too ambiguous, but rather that the proposal on the whole is contradictory. Consequently, given the brevity of the micro-management argument and the implicit concession on vagueness, it appears that there is no serious argument the Proposal improperly "probes too deeply". Rather the correct conclusion is that the Proposal in fact seeks a "reasonable level of detail" such that shareholders are in a position to make an informed judgment.

5. Political process: the Proposal is proper because it does not seek an evaluation of a specific

legislative proposal.

Finally, the Company makes a brief argument that the Proposal involves the Company in the political or legislative process by asking the Company to evaluate the impact that the Programs would have on the company's business operations. To support this contention the Company points to three cases *International Business Machines Corp.* (March 2, 2000); *Electronic Data Systems Corp.* (March 24, 2000) and *Niagara Mohawk Holding, Inc.* (March 5, 2001). One does not need to go any farther than looking at the text of these proposals to see that they do not apply to this case. The proposal in *International Business Machines Corp.* (which is reflective of the other two) requests:

the Board of Directors to establish a committee of outside directors to prepare a report at reasonable expense to shareholders on the potential impact on the Company of pension-related proposals now being considered by national policy makers, including issues under review by federal regulators about the legality of cash balance pension plan conversions under federal anti-discrimination laws, as well as legislative proposals affecting cash balance plan conversions and related issues.

As this makes clear, that proposal expressly sought a direct evaluation of specific legislative and regulatory proposals concerning cash balance plan conversions. The Proposal is quite distinct from the *International Business Machines Corp.* type proposal because it does not seek an evaluation, expressly or implicitly, of *any* legislative or regulatory proposals let alone a specific proposal comparable to "cash balance pension plan conversions under federal anti-discrimination laws".

It is also evident that some proposals which *do* involve companies in the political or legislative process are in fact permissible. Consider, *Coca-Cola Company* (February 2, 2000), in which the SEC staff denied a no-action request. In that case, the resolution asked the company to promote the retention and development of bottle deposit systems and laws. It also requested the company cease any efforts to replace existing deposit and return systems with one-way containers in developing countries or countries that do not have an effective and comprehensive municipal trash collection and disposal system. And in *Johnson and Johnson* (January 13, 2005) the shareholder requested the company to, inter alia, "Petition the relevant regulatory agencies requiring safety testing for the Company's products to accept as total replacements for animal-based methods, those approved non-animal methods described above, along with any others currently used and accepted by the Organization for Economic Cooperation and Development (OECD) and other developed countries." That proposal was deemed permissible in the face of a "political process" objection. See also, *RJR Nabisco Holdings Corp* (February 13, 1998) (proposal requesting "management to implement the same programs that we have voluntarily proposed and adopted in the United States to prevent youth from smoking and buying our cigarettes in developing countries." was permissible.)

Finally, we note that significant social policy issues inherently have a political aspect to them. Because such issues are important to society and have a high public profile, they attract the attention of politicians and legislators. Consequently, any ordinary business analysis must take this inherently political characteristic of significant policy issues into account. Thus when we see that the privacy of customer telephone records and communication content is, not surprisingly, a political issue we should recognize that it is not fatal to our Proposal. Therefore, we urge the Staff not to conclude the Proposal is excludable as ordinary business.

6. "Touches" on a Significant Policy Issue: The Proposal must appear on the Company proxy because it directly and fully raises a Significant Policy Issue.

In the last section of its letter, the Company seems to have forgotten two seminal cases in Rule 14a-8 law - *Roosevelt v. E.I. DuPont de Nemours & Company*, 958 F. 2d 416 (DC Cir. 1992) and *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877 (S.D.N.Y. 1993). These cases make it abundantly clear that "***the proposal may be excluded only after the proposal is also found to raise no substantial policy consideration.***" *Id* at 891. First, to argue that the proposal can be excluded, as stated by the Company, "regardless of whether or not it touches upon a significant social policy issue" is directly contrary to this rule.

Second, as was discussed at length earlier, it is clear that AT&T is currently facing a significant social policy issue in the form of its alleged participation in the Programs and widespread concerns about privacy. To imply that the Proposal merely touches on a significant policy issue is misplaced and cannot provide sufficient reasons to overcome the Company's significant burden of persuasion to exclude the Proposal.

III. Vagueness: The Proposal does not violate the law and has struck the proper balance between specificity and generality, therefore the Company has the power and authority to implement it.

The Company's final argument is that the Proposal is vague and indefinite and, therefore, the Company would lack the power or authority to implement it. Essentially, they contend that if the Company issued the requested report that "it would issue a report excluding substantially all of the information sought for by the Proposal." They also claim that this makes the Proposal internally self-conflicting and therefore so vague and ambiguous that it is beyond the Company's "power to effectuate" in violation of Rule 14a-8(i)(6). Both claims are built upon the premise that the state secrets privilege makes any discussion of the overarching issues forbidden and therefore the Proposal has irreconcilable conflicts within its requests that would result in a meaningless or empty report.

First, as discussed at the beginning of this letter the state secrets objection does not make the Proposal excludable. Therefore, it is inaccurate to say that the essential portion of the information requested by the Proposal would be identified by a court as classified information and therefore must be treated as confidential. As explained above, the existence of the Programs and the Company's participation has already been established in court and requesting an overarching discussion of these issues does not violate the law. Therefore, if the Proposal were implemented it would contain information that is useful and relevant for shareholders. As such, shareholders are not being misled by the language of the Proposal nor does it promise more information than can be delivered. The Proposal seeks a general discussion of the privacy issues confronting the Company and the Company will be able to have such a discussion.

Furthermore, to suggest that shareholders can not understand the confidentiality requirements that would be necessary to implement the Proposal is to vastly underestimate the intelligence of shareholders. Many of AT&T's shareholders are large institutional investors who receive the counsel of professional proxy advisors and are more than familiar with the demands of confidentiality requirements. In addition, the Proposal makes clear, in the face of the Company's vigorous attempts to

find to the contrary, that it is not seeking a high level of specificity or intricate detail. In fact, shareholders will be able understand that the Proposal requests a general discussion of the issues and does not seek to illicit confidential information.

Turning to the cases cited by the Company, it is evident that, once again, they do not apply to the Proposal and simply document the general proposition that proposals may not be vague, indefinite or beyond the power of the company to effectuate. In *Philadelphia Electric Co.* (July 30, 1992) the proposal sought a plan “that will in some measure equate with the gratuities bestowed on Management”. It is self-evident why that proposal was excluded as vague and we observe that, as the Staff concluded, reading the full proposal did not shed sufficient light on the meaning of the proposal.

Faqua Industries (March 12, 1991) presents a different case in which the “meaning and application of [specific] terms and conditions . . . would be subject to differing interpretations.” If the argument being made by the Company that this Proposal contains terms that are subject to differing interpretations, it has not made the argument beyond the unsupported and unexplained statement that “the terms of the Proposal are vague and ambiguous.” The Company has not argued, for example, that the meaning of the words “communications” or “privacy” need to be defined. Consequently, the facts in *Faqua* is not analogous to the Proposal.

As the Company rightly pointed out, the proposal in *International Business Machines Corporation* (January 14, 1992) was properly excluded because its resolve clause, in its entirety, stated “It is now apparent that the need for representation has become a necessity”. This is a clear example of an excessively vague proposal because it only contains conclusory language and does not ask the company to do anything in particular. In contrast, the Proposal, sets forth a series of topics we would like to see the Company address. The topics (the overarching issues surrounding disclosure of customer communications; additional policies to protect customer communications; and past costs associated with the allegations) are described with a reasonable, but not excessive, level of detail that gives shareholders a clear sense of what is being asked. Because our Proposal is distinct from the *International Business Machines Corporation* proposal, this case does not provide a basis for exclusion.

Similar to *Faqua*, the company's argument in *The Southern Company* (February 23, 1995) was that the “proposal is replete with vague and indefinite terms, such as “essential steps”, “highest standards”, “positive steps”, “reliable information”, and “grave deficiencies”. Once, again that argument and, in this case, *The Southern Company* is not applicable to the Proposal.

In contrast there are numerous analogous cases in which proposals were not excluded as being so vague as to make implementation impossible.

In *Microsoft Corporation* (September 14, 2000) the proposal requested the board “to make all possible lawful efforts to implement and/or increase activity on each of the (human rights) principles named above in the People's Republic of China.” The company argued that the proposal was too vague to implement since it was merely a broad statement of values with no discussion of concrete implementation methods. The Staff rejected this argument and concluded that the company could not exclude the proposal. Like *Microsoft*, the Proposal is focused on asking the Company to address questions of how the Company's activities impact fundamental individual rights and liberties. Similarly, the Proposal provides a reasonable level of specificity regarding those rights and is therefore

permissible.

The *Kroger Co.* (April 12, 2000) proposal called for the company to adopt a policy of removing “genetically engineered” products from its private label products, labeling and identifying products that may contain a genetically engineered organism, and reporting to shareholders. The company challenged the proposal on many grounds including the argument that the term “genetically engineered” was not defined in the proposal and was the subject of competing definitions. Despite the lack of a definition or a consensus on the meaning of the terms, the Staff rejected the lack of definition argument and concluded that the proposal was permissible. The company also claimed that because state law required that labeling not be untrue, deceptive or misleading that if it labeled its products as sought by the proposal it could be subject to potential liability due to the fact that company did not have the basic information that might be required on the label. The proponent in that case argued that the labeling issue could be overcome by placing a label stating that a product did — or did not — contain any genetically engineered material.

In our Proposal we are confronted with a similar argument. First, even in the context of a heated debate about the meaning of the words “genetically engineered”, the Staff did not require a definition of the term, but allowed common sense to guide shareholders. Second, as explained in length earlier, it is evident from court proceedings and the plain language of the Proposal that the Company will be able to provide a general level discussion of the privacy issues raised by the media reports and lawsuits without violating the law. We have pointed to language already used by the Company and have provided our own suggestions about how to strike a reasonable balance between confidentiality concerns and the needs of shareholders to engage management on this significant social policy issue.

Finally, in *Bristol-Myers Squibb Company* (April 3, 2000) the proposal asked the board to implement a policy of price restraint on pharmaceutical products for individual customers and institutional purchasers to keep drug prices at reasonable levels and prepare a report to shareholders on any changes in its current pricing policy. The company argued that it was unable to implement the proposal because the proposal did not define the term “reasonable levels”. It also claimed that even if the company implemented the proposal, it could not determine when a “reasonable level” would be reached. The proponent responded by arguing that the proposal simply sought a policy of price restraint, and that such a concept was readily understandable. The Staff concurred with the proponent concluding that Rule 14a-8(i)(3) could not be a basis for exclusion. As in *Bristol-Myers Squibb Company*, the Proponents have addressed the issue in a reasonable fashion. There is no need to create ambiguities where none exist.

Returning to the basic premise of the Company's argument that the state secrets privilege will make the Proposal impossible to implement, as was made very clear earlier in this letter, the Company is in a position to speak about the issues raised in the Proposal in general terms. The Hon. Judge Walker has concluded that the existence of the Programs and AT&T's participation is not a secret. As such, the Company can implement the Proposal and respect the needs on confidentiality without misleading shareholders, violating the law or creating a meaningless report. As such, Rules 14a-8(i)(3) and 14a-8(i)(6) do not apply and cannot be a basis for excluding the Proposal.

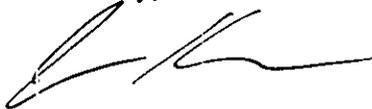
Conclusion

In conclusion, I respectfully request the Staff to inform the Company that Rule 14a-8 requires denial of

the Company's no-action request. As demonstrated above, the Proposal is not excludible under any of the criteria of Rule 14a-8. Not only does the Proposal raise a critical social policy issue facing the nation and the Company, but it raises that issue in a manner that does not cause the Company to violate the law nor does it mislead shareholders. In the event that the Staff should decide to concur with the Company and issue a no-action letter, I respectfully request the opportunity to speak with the Staff and, as did the Company, ask that the decision be immediately appealed to the full Commission.

Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jonas Kron', written in a cursive style.

Jonas Kron
Attorney at Law

Enclosures

cc: Wayne A. Wirtz, Assistant General Counsel, Legal Department, AT&T Inc.

Exhibits

1. *Judge Vaugh R. Walker's July 20, 2006 Order in Hepting v. AT&T Corporation.*
2. John O'Neil and Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained*, New York Times, May 12, 2006.
3. FoxNews: *Verizon- We Didn't Give Customers' Call Records to NSA Either*, May 16, 2006.
4. May 2006 Gallup Poll.
5. December 2005 Rasmussen Report Poll.
6. List of media reports.
7. Statement of Federal Communications Commissioner Michael Copps.
8. May 15, 2006 letter from Representative Edward Markey (D- MA).
9. *Petition of Vermont Department of Public Service Docket No. 7193.*
10. *ACLU of Pennsylvania v. AT&T Communications of PA, LLC, et al.*
11. Scott Lindlaw, *SF Reviews Contracts with AT&T Over Domestic Spying*, Associated Press, July 11, 2006.
12. Ryan Singel, *AT&T Sued Over NSA Eavesdropping*, Wired, January 31, 2006.
13. May 2006 Newsweek Poll.
14. Boston Common Asset Press Release.

EXHIBIT 1

- 1 (2) Section 109 of Title I of the Foreign Intelligence
2 Surveillance Act of 1978 (FISA), 50 USC § 1809, by
3 engaging in illegal electronic surveillance of
4 plaintiffs' communications under color of law;
- 5 (3) Section 802 of Title III of the Omnibus Crime Control and
6 Safe Streets Act of 1968, as amended by section 101 of
7 Title I of the Electronic Communications Privacy Act of
8 1986 (ECPA), 18 USC §§ 2511(1)(a), (1)(c), (1)(d) and
9 (3)(a), by illegally intercepting, disclosing, using
10 and/or divulging plaintiffs' communications;
- 11 (4) Section 705 of Title VII of the Communications Act of
12 1934, as amended, 47 USC § 605, by unauthorized
13 divulgence and/or publication of plaintiffs'
14 communications;
- 15 (5) Section 201 of Title II of the ECPA ("Stored
16 Communications Act"), as amended, 18 USC §§ 2702(a)(1)
17 and (a)(2), by illegally divulging the contents of
18 plaintiffs' communications;
- 19 (6) Section 201 of the Stored Communications Act, as amended
20 by section 212 of Title II of the USA PATRIOT Act, 18 USC
21 § 2702(a)(3), by illegally divulging records concerning
22 plaintiffs' communications to a governmental entity and
- 23 (7) California's Unfair Competition Law, Cal Bus & Prof Code
24 §§ 17200 et seq, by engaging in unfair, unlawful and
25 deceptive business practices.

26 The complaint seeks certification of a class action and redress
27 through statutory damages, punitive damages, restitution,
28 disgorgement and injunctive and declaratory relief.

1 On April 5, 2006, plaintiffs moved for a preliminary
2 injunction seeking to enjoin defendants' allegedly illegal
3 activity. Doc #30 (MPI). Plaintiffs supported their motion by
4 filing under seal three documents, obtained by former AT&T
5 technician Mark Klein, which allegedly demonstrate how AT&T has
6 implemented a warrantless surveillance system on behalf of the NSA
7 at a San Francisco AT&T facility. Doc #31, Exs A-C (the "AT&T
8 documents"). Plaintiffs also filed under seal supporting
9 declarations from Klein (Doc #31) and J Scott Marcus (Doc #32), a
10 putative expert who reviewed the AT&T documents and the Klein
11 declaration.

12 On April 28, 2006, AT&T moved to dismiss this case. Doc
13 #86 (AT&T MTD). AT&T contends that plaintiffs lack standing and
14 were required but failed to plead affirmatively that AT&T did not
15 receive a government certification pursuant to 18 USC §
16 2511(2)(a)(ii)(B). AT&T also contends it is entitled to statutory,
17 common law and qualified immunity.

18 On May 13, 2006, the United States moved to intervene as
19 a defendant and moved for dismissal or, alternatively, for summary
20 judgment based on the state secrets privilege. Doc #124-1 (Gov
21 MTD). The government supported its assertion of the state secrets
22 privilege with public declarations from the Director of National
23 Intelligence, John D Negroponte (Doc #124-2 (Negroponte Decl)), and
24 the Director of the NSA, Keith B Alexander (Doc #124-3 (Alexander
25 Decl)), and encouraged the court to review additional classified
26 submissions *in camera* and *ex parte*. The government also asserted
27 two statutory privileges under 50 USC § 402 note and 50 USC § 403-
28 1(i)(1).

1 surveillance activities. Finally, the court addresses the
2 statutory privileges raised by the government.

3
4 A

5 "The state secrets privilege is a common law evidentiary
6 rule that protects information from discovery when disclosure would
7 be inimical to the national security. Although the exact origins
8 of the privilege are not certain, the privilege in this country has
9 its initial roots in Aaron Burr's trial for treason, and has its
10 modern roots in United States v Reynolds, 345 US 1 (1953)." In re
11 United States, 872 F2d 472, 474-75 (DC Cir 1989) (citations omitted
12 and altered). In his trial for treason, Burr moved for a *subpoena*
13 *duces tecum* ordering President Jefferson to produce a letter by
14 General James Wilkinson. United States v Burr, 25 F Cas 30, 32
15 (CCD Va 1807). Responding to the government's argument "that the
16 letter contains material which ought not to be disclosed," Chief
17 Justice Marshall riding circuit noted, "What ought to be done under
18 such circumstances presents a delicate question, the discussion of
19 which, it is hoped, will never be rendered necessary in this
20 country." *Id* at 37. Although the court issued the subpoena, *id* at
21 37-38, it noted that if the letter "contain[s] any matter which it
22 would be imprudent to disclose, which it is not the wish of the
23 executive to disclose, such matter, if it be not immediately and
24 essentially applicable to the point, will, of course, be
25 suppressed." *Id* at 37.

26 //

27 //

28 //

1 The actions of another president were at issue in Totten
2 v United States, 92 US 105 (1876), in which the Supreme Court
3 established an important precursor to the modern-day state secrets
4 privilege. In that case, the administrator of a former spy's
5 estate sued the government based on a contract the spy allegedly
6 made with President Lincoln to recover compensation for espionage
7 services rendered during the Civil War. Id at 105-06. The Totten
8 Court found the action to be barred:

9 The service stipulated by the contract was a secret
10 service; the information sought was to be obtained
11 clandestinely, and was to be communicated
12 privately; the employment and the service were to
13 be equally concealed. Both employer and agent must
14 have understood that the lips of the other were to
15 be for ever sealed respecting the relation of
16 either to the matter. This condition of the
17 engagement was implied from the nature of the
18 employment, and is implied in all secret
19 employments of the government in time of war, or
20 upon matters affecting our foreign relations, where
21 a disclosure of the service might compromise or
22 embarrass our government in its public duties, or
23 endanger the person or injure the character of the
24 agent.

25 Id at 106, quoted in Tenet v Doe, 544 US 1, 7-8 (2005). Hence,
26 given the secrecy implied in such a contract, the Totten Court
27 "thought it entirely incompatible with the nature of such a
28 contract that a former spy could bring suit to enforce it." Tenet,
544 US at 8. Additionally, the Totten Court observed:

29 It may be stated as a general principle, that
30 public policy forbids the maintenance of any suit
31 in a court of justice, the trial of which would
32 inevitably lead to the disclosure of matters which
33 the law itself regards as confidential, and
34 respecting which it will not allow the confidence
35 to be violated. * * * Much greater reason exists
36 for the application of the principle to cases of
37 contract for secret services with the government,
38 as the existence of a contract of that kind is
itself a fact not to be disclosed.

1 Totten, 92 US at 107. Characterizing this aspect of Totten, the
2 Supreme Court has noted, "No matter the clothing in which alleged
3 spies dress their claims, Totten precludes judicial review in cases
4 such as [plaintiffs'] where success depends upon the existence of
5 their secret espionage relationship with the Government." Tenet,
6 544 US at 8. "Totten's core concern" is "preventing the existence
7 of the [alleged spy's] relationship with the Government from being
8 revealed." Id at 10.

9 In the Cold War era case of Reynolds v United States, 345
10 US 1 (1953), the Supreme Court first articulated the state secrets
11 privilege in its modern form. After a B-29 military aircraft
12 crashed and killed three civilian observers, their widows sued the
13 government under the Federal Tort Claims Act and sought discovery
14 of the Air Force's official accident investigation. Id at 2-3.
15 The Secretary of the Air Force filed a formal "Claim of Privilege"
16 and the government refused to produce the relevant documents to the
17 court for *in camera* review. Id at 4-5. The district court deemed
18 as established facts regarding negligence and entered judgment for
19 plaintiffs. Id at 5. The Third Circuit affirmed and the Supreme
20 Court granted certiorari to determine "whether there was a valid
21 claim of privilege under [FRCP 34]." Id at 6. Noting this
22 country's theretofore limited judicial experience with "the
23 privilege which protects military and state secrets," the court
24 stated:

25 //

26 //

27 //

28 //

1 The privilege belongs to the Government and must be
2 asserted by it * * *. It is not to be lightly
3 invoked. There must be a formal claim of
4 privilege, lodged by the head of the department
5 which has control over the matter, after actual
6 personal consideration by that officer. The court
itself must determine whether the circumstances are
appropriate for the claim of privilege, and yet do
so without forcing a disclosure of the very thing
the privilege is designed to protect.

7 Id at 7-8 (footnotes omitted). The latter determination requires a
8 "formula of compromise," as "[j]udicial control over the evidence
9 in a case cannot be abdicated to the caprice of executive
10 officers," yet a court may not "automatically require a complete
11 disclosure to the judge before the claim of privilege will be
12 accepted in any case." Id at 9-10. Striking this balance, the
13 Supreme Court held that the "occasion for the privilege is
14 appropriate" when a court is satisfied "from all the circumstances
15 of the case, that there is a reasonable danger that compulsion of
16 the evidence will expose military matters which, in the interest of
17 national security, should not be divulged." Id at 10.

18 The degree to which the court may "probe in satisfying
19 itself that the occasion for invoking the privilege is appropriate"
20 turns on "the showing of necessity which is made" by plaintiffs.
21 Id at 11. "Where there is a strong showing of necessity, the claim
22 of privilege should not be lightly accepted, but even the most
23 compelling necessity cannot overcome the claim of privilege if the
24 court is ultimately satisfied that military secrets are at stake."
25 Id. Finding both a "reasonable danger that the accident
26 investigation report would contain" state secrets and a "dubious
27 showing of necessity," the court reversed the Third Circuit's
28 decision and sustained the claim of privilege. Id at 10-12.

1 In Halkin v Helms, 598 F2d 1 (DC Cir 1978) (Halkin I),
2 the District of Columbia Circuit applied the principles enunciated
3 in Reynolds in an action alleging illegal NSA wiretapping. Former
4 Vietnam War protestors contended that "the NSA conducted
5 warrantless interceptions of their international wire, cable and
6 telephone communications" at the request of various federal
7 defendants and with the cooperation of telecommunications
8 providers. Id at 3. Plaintiffs challenged two separate NSA
9 operations: operation MINARET, which was "part of [NSA's] regular
10 signals intelligence activity in which foreign electronic signals
11 were monitored," and operation SHAMROCK, which involved "processing
12 of all telegraphic traffic leaving or entering the United States."
13 Id at 4.

14 The government moved to dismiss on state secrets grounds,
15 arguing that civil discovery would impermissibly "(1) confirm the
16 identity of individuals or organizations whose foreign
17 communications were acquired by NSA, (2) disclose the dates and
18 contents of such communications, or (3) divulge the methods and
19 techniques by which the communications were acquired by NSA." Id
20 at 4-5. After plaintiffs "succeeded in obtaining a limited amount
21 of discovery," the district court concluded that plaintiffs' claims
22 challenging operation MINARET could not proceed because "the
23 ultimate issue, the fact of acquisition, could neither be admitted
24 nor denied." Id at 5. The court denied the government's motion to
25 dismiss on claims challenging operation SHAMROCK because the court
26 "thought congressional committees investigating intelligence
27 matters had revealed so much information about SHAMROCK that such a
28 disclosure would pose no threat to the NSA mission." Id at 10.

1 On certified appeal, the District of Columbia Circuit
2 noted that even "seemingly innocuous" information is privileged if
3 that information is part of a classified "mosaic" that "can be
4 analyzed and fitted into place to reveal with startling clarity how
5 the unseen whole must operate." Id at 8. The court affirmed
6 dismissal of the claims related to operation MINARET but reversed
7 the district court's rejection of the privilege as to operation
8 SHAMROCK, reasoning that "confirmation or denial that a particular
9 plaintiff's communications have been acquired would disclose NSA
10 capabilities and other valuable intelligence information to a
11 sophisticated intelligence analyst." Id at 10. On remand, the
12 district court dismissed plaintiffs' claims against the NSA and
13 individuals connected with the NSA's alleged monitoring.

14 Plaintiffs were left with claims against the Central Intelligence
15 Agency (CIA) and individuals who had allegedly submitted watchlists
16 to the NSA on the presumption that the submission resulted in
17 interception of plaintiffs' communications. The district court
18 eventually dismissed the CIA-related claims as well on state
19 secrets grounds and the case went up again to the court of appeals.

20 The District of Columbia Circuit stated that the state
21 secrets inquiry "is not a balancing of ultimate interests at stake
22 in the litigation," but rather "whether the showing of the harm
23 that might reasonably be seen to flow from disclosure is adequate
24 in a given case to trigger the absolute right to withhold the
25 information sought in that case." Halkin v Helms, 690 F2d 977, 990
26 (DC Cir 1982) (Halkin II). The court then affirmed dismissal of
27 "the claims for injunctive and declaratory relief against the CIA
28 defendants based upon their submission of plaintiffs' names on

1 'watchlists' to NSA." Id at 997 (emphasis omitted). The court
2 found that plaintiffs lacked standing given the court's "ruling in
3 Halkin I that evidence of the fact of acquisition of plaintiffs'
4 communications by NSA cannot be obtained from the government, nor
5 can such fact be presumed from the submission of watchlists to that
6 Agency." Id at 999 (emphasis omitted).

7 In Ellsberg v Mitchell, 709 F2d 51 (DC Cir 1983), the
8 District of Columbia Circuit addressed the state secrets privilege
9 in another wiretapping case. Former defendants and attorneys in
10 the "Pentagon Papers" criminal prosecution sued individuals who
11 allegedly were responsible for conducting warrantless electronic
12 surveillance. Id at 52-53. In response to plaintiffs'
13 interrogatories, defendants admitted to two wiretaps but refused to
14 answer other questions on the ground that the requested information
15 was privileged. Id at 53. The district court sustained the
16 government's formal assertion of the state secrets privilege and
17 dismissed plaintiffs' claims pertaining to foreign communications
18 surveillance. Id at 56.

19 On appeal, the District of Columbia Circuit noted that
20 "whenever possible, sensitive information must be disentangled from
21 nonsensitive information to allow for the release of the latter."
22 Id at 57. The court generally affirmed the district court's
23 decisions regarding the privilege, finding "a 'reasonable danger'
24 that revelation of the information in question would either enable
25 a sophisticated analyst to gain insights into the nation's
26 intelligence-gathering methods and capabilities or would disrupt
27 diplomatic relations with foreign governments." Id at 59. The
28 court disagreed with the district court's decision that the

1 privilege precluded discovery of the names of the attorneys general
2 that authorized the surveillance. Id at 60.

3 Additionally, responding to plaintiffs' argument that the
4 district court should have required the government to disclose more
5 fully its basis for asserting the privilege, the court recognized
6 that "procedural innovation" was within the district court's
7 discretion and noted that "[t]he government's public statement need
8 be no more (and no less) specific than is practicable under the
9 circumstances." Id at 64.

10 In considering the effect of the privilege, the court
11 affirmed dismissal "with regard to those [individuals] whom the
12 government ha[d] not admitted overhearing." Id at 65. But the
13 court did not dismiss the claims relating to the wiretaps that the
14 government had conceded, noting that there was no reason to
15 "suspend the general rule that the burden is on those seeking an
16 exemption from the Fourth Amendment warrant requirement to show the
17 need for it." Id at 68.

18 In Kasza v Browner, 133 F3d 1159 (9th Cir 1998), the
19 Ninth Circuit issued its definitive opinion on the state secrets
20 privilege. Former employees at a classified United States Air
21 Force facility brought a citizen suit under the Resource
22 Conservation and Recovery Act (RCRA), 42 USC § 6972, alleging the
23 Air Force violated that act. Id at 1162. The district court
24 granted summary judgment against plaintiffs, finding discovery of
25 information related to chemical inventories impossible due to the
26 state secrets privilege. Id. On appeal, plaintiffs argued that an
27 exemption in the RCRA preempted the state secrets privilege and
28 even if not preempted, the privilege was improperly asserted and

1 too broadly applied. Id at 1167-69. After characterizing the
2 state secrets privilege as a matter of federal common law, the
3 Ninth Circuit recognized that "statutes which invade the common law
4 * * * are to be read with a presumption favoring the retention of
5 long-established and familiar principles, except when a statutory
6 purpose to the contrary is evident." Id at 1167 (omissions in
7 original) (citations omitted). Finding no such purpose, the court
8 held that the statutory exemption did not preempt the state secrets
9 privilege. Id at 1168.

10 Kasza also explained that the state secrets privilege can
11 require dismissal of a case in three distinct ways. "First, by
12 invoking the privilege over particular evidence, the evidence is
13 completely removed from the case. The plaintiff's case then goes
14 forward based on evidence not covered by the privilege. * * * If,
15 after further proceedings, the plaintiff cannot prove the *prima*
16 *facie* elements of her claim with nonprivileged evidence, then the
17 court may dismiss her claim as it would with any plaintiff who
18 cannot prove her case." Id at 1166. Second, "if the privilege
19 deprives the defendant of information that would otherwise give the
20 defendant a valid defense to the claim, then the court may grant
21 summary judgment to the defendant." Id (internal quotation
22 omitted) (emphasis in original). Finally, and most relevant here,
23 "notwithstanding the plaintiff's ability to produce nonprivileged
24 evidence, if the 'very subject matter of the action' is a state
25 secret, then the court should dismiss the plaintiff's action based
26 solely on the invocation of the state secrets privilege." Id
27 (quoting Reynolds, 345 US at 11 n26). See also Reynolds, 345 US at
28 11 n26 (characterizing Totten as a case "where the very subject

1 matter of the action, a contract to perform espionage, was a matter
2 of state secret. The action was dismissed on the pleadings without
3 ever reaching the question of evidence, since it was so obvious
4 that the action should never prevail over the privilege.”).

5 According the “utmost deference” to the government’s
6 claim of privilege and noting that even “seemingly innocuous
7 information” could be “part of a classified mosaic,” *id* at 1166,
8 Kasza concluded after *in camera* review of classified declarations
9 “that release of such information would reasonably endanger
10 national security interests.” *Id* at 1170. Because “no protective
11 procedure” could salvage plaintiffs’ case, and “the very subject
12 matter of [her] action [was] a state secret,” the court affirmed
13 dismissal. *Id*.

14 More recently, in Tenet v Doe, 544 US 1 (2005), the
15 Supreme Court reaffirmed Totten, holding that an alleged former
16 Cold War spy could not sue the government to enforce its
17 obligations under a covert espionage agreement. *Id* at 3.
18 Importantly, the Court held that Reynolds did not “replac[e] the
19 categorical Totten bar with the balancing of the state secrets
20 evidentiary privilege in the distinct class of cases that depend
21 upon clandestine spy relationships.” *Id* at 9-10.

22 Even more recently, in El-Masri v Tenet, 2006 WL 1391390,
23 05-cv-01417 (ED Va May 12, 2006), plaintiff sued the former
24 director of the CIA and private corporations involved in a program
25 of “extraordinary rendition,” pursuant to which plaintiff was
26 allegedly beaten, tortured and imprisoned because the government
27 mistakenly believed he was affiliated with the al Qaeda terrorist
28 organization. *Id* at *1-2. The government intervened “to protect

1 its interests in preserving state secrets." Id at *3. The court
2 sustained the government's assertion of the privilege:

3 [T]he substance of El-Masri's publicly available
4 complaint alleges a clandestine intelligence
5 program, and the means and methods the foreign
6 intelligence services of this and other countries
7 used to carry out the program. And, as the public
8 declaration makes pellucidly clear, any admission
9 or denial of these allegations by defendants * * *
10 would present a grave risk of injury to national
11 security.

12 Id at *5. The court also rejected plaintiff's argument "that
13 government officials' public affirmation of the existence" of the
14 rendition program somehow undercut the claim of privilege because
15 the government's general admission provided "no details as to the
16 [program's] means and methods," which were "validly claimed as
17 state secrets." Id. Having validated the exercise of privilege,
18 the court reasoned that dismissal was required because "any answer
19 to the complaint by the defendants risk[ed] the disclosure of
20 specific details [of the program]" and special discovery procedures
21 would have been "plainly ineffective where, as here, the entire aim
22 of the suit [was] to prove the existence of state secrets." Id at
23 *6.

24 B

25 Relying on Kasza, the government advances three reasons
26 why the state secrets privilege requires dismissing this action or
27 granting summary judgment for AT&T: (1) the very subject matter of
28 this case is a state secret; (2) plaintiffs cannot make a *prima*
facie case for their claims without classified evidence and (3) the
privilege effectively deprives AT&T of information necessary to
raise valid defenses. Doc #245-1 (Gov Reply) at 3-5.

1 In support of its contention that the very subject matter
2 of this action is a state secret, the government argues: "AT&T
3 cannot even confirm or deny the key factual premise underlying
4 [p]laintiffs' entire case — that AT&T has provided any assistance
5 whatsoever to NSA regarding foreign-intelligence surveillance.
6 Indeed, in the formulation of Reynolds and Kasza, that allegation
7 is 'the very subject of the action.'" Id at 4-5.

8 Additionally, the government claims that dismissal is
9 appropriate because plaintiffs cannot establish a *prima facie* case
10 for their claims. Contending that plaintiffs "persistently confuse
11 speculative allegations and untested assertions for established
12 facts," the government attacks the Klein and Marcus declarations
13 and the various media reports that plaintiffs rely on to
14 demonstrate standing. Id at 4. The government also argues that
15 "[e]ven when alleged facts have been the 'subject of widespread
16 media and public speculation' based on '[u]nofficial leaks and
17 public surmise,' those alleged facts are not actually established
18 in the public domain." Id at 8 (quoting Afshar v Dept of State,
19 702 F2d 1125, 1130-31 (DC Cir 1983)).

20 The government further contends that its "privilege
21 assertion covers any information tending to confirm or deny (a) the
22 alleged intelligence activities, (b) whether AT&T was involved with
23 any such activity, and (c) whether a particular individual's
24 communications were intercepted as a result of any such activity."
25 Gov MTD at 17-18. The government reasons that "[w]ithout these
26 facts * * * [p]laintiffs ultimately will not be able to prove
27 injury-in-fact and causation," thereby justifying dismissal of this
28 action for lack of standing. Id at 18.

1 The government also notes that plaintiffs do not fall
2 within the scope of the publicly disclosed "terrorist surveillance
3 program" (see *infra* I(C)(1)) because "[p]laintiffs do not claim to
4 be, or to communicate with, members or affiliates of [the] al Qaeda
5 [terrorist organization] — indeed, [p]laintiffs expressly exclude
6 from their purported class any foreign powers or agent of foreign
7 powers * * *." *Id* at 18 n9 (citing FAC, ¶ 70). Hence, the
8 government concludes the named plaintiffs "are in no different
9 position from any other citizen or AT&T subscriber who falls
10 outside the narrow scope of the [terrorist surveillance program]
11 but nonetheless disagrees with the program." *Id* (emphasis in
12 original).

13 Additionally, the government contends that plaintiffs'
14 Fourth Amendment claim fails because no warrant is required for the
15 alleged searches. In particular, the government contends that the
16 executive has inherent constitutional authority to conduct
17 warrantless searches for foreign intelligence purposes, *id* at 24
18 (citing *In re Sealed Case*, 310 F3d 717, 742 (For Intel Surv Ct of
19 Rev 2002)), and that the warrant requirement does not apply here
20 because this case involves "special needs" that go beyond a routine
21 interest in law enforcement, *id* at 26. Accordingly, to make a
22 *prima facie* case, the government asserts that plaintiffs would have
23 to demonstrate that the alleged searches were unreasonable, which
24 would require a fact-intensive inquiry that the government contends
25 plaintiffs could not perform because of the asserted privilege. *Id*
26 at 26-27.

27 //

28 //

1 The government also argues that plaintiffs cannot
2 establish a *prima facie* case for their statutory claims because
3 plaintiffs must prove "that any alleged interception or disclosure
4 was not authorized by the Government." The government maintains
5 that "[p]laintiffs bear the burden of alleging and proving the lack
6 of such authorization," *id* at 21-22, and that they cannot meet that
7 burden because "information confirming or denying AT&T's
8 involvement in alleged intelligence activities is covered by the
9 state secrets assertion." *Id* at 23.

10 Because "the existence or non-existence of any
11 certification or authorization by the Government relating to any
12 AT&T activity would be information tending to confirm or deny
13 AT&T's involvement in any alleged intelligence activity," Doc #145-
14 1 (Gov 5/17/06 Br) at 17, the government contends that its state
15 secrets assertion precludes AT&T from "present[ing] the facts that
16 would constitute its defenses." Gov Reply at 1. Accordingly, the
17 government also argues that the court could grant summary judgment
18 in favor of AT&T on that basis.

19
20 C

21 The first step in determining whether a piece of
22 information constitutes a "state secret" is determining whether
23 that information actually is a "secret." Hence, before analyzing
24 the application of the state secrets privilege to plaintiffs'
25 claims, the court summarizes what has been publicly disclosed about
26 NSA surveillance programs as well as the AT&T documents and
27 accompanying Klein and Marcus declarations.

28 //

2 Within the last year, public reports have surfaced on at
3 least two different types of alleged NSA surveillance programs,
4 neither of which relies on warrants. The New York Times disclosed
5 the first such program on December 16, 2005. Doc #19 (Cohn Decl),
6 Ex J (James Risen and Eric Lichtblau, *Bush Lets US Spy on Callers*
7 *Without Courts*, The New York Times (Dec 16, 2005)). The following
8 day, President George W Bush confirmed the existence of a
9 "terrorist surveillance program" in his weekly radio address:

10 In the weeks following the [September 11, 2001]
11 terrorist attacks on our Nation, I authorized the
12 National Security Agency, consistent with US law
13 and the Constitution, to intercept the
14 international communications of people with known
15 links to Al Qaeda and related terrorist
16 organizations. Before we intercept these
17 communications, the Government must have
18 information that establishes a clear link to these
19 terrorist networks.

20 Doc #20 (Pl. Request for Judicial Notice), Ex 1 at 2, available at
21 <http://www.whitehouse.gov/news/releases/2005/12/print/20051217.html>
22 (last visited July 19, 2006). The President also described the
23 mechanism by which the program is authorized and reviewed:

24 The activities I authorized are reviewed
25 approximately every 45 days. Each review is based
26 on a fresh intelligence assessment of terrorist
27 threats to the continuity of our Government and the
28 threat of catastrophic damage to our homeland.
During each assessment, previous activities under
the authorization are reviewed. The review
includes approval by our Nation's top legal
officials, including the Attorney General and the
Counsel to the President. I have reauthorized this
program more than 30 times since the September the
11th attacks, and I intend to do so for as long as
our Nation faces a continuing threat from Al Qaeda
and related groups.

//

//

1 The NSA's activities under this authorization are
2 thoroughly reviewed by the Justice Department and
3 NSA's top legal officials, including NSA's General
4 Counsel and Inspector General. Leaders in Congress
5 have been briefed more than a dozen times on this
6 authorization and the activities conducted under
7 it. Intelligence officials involved in this
8 activity also receive extensive training to ensure
9 they perform their duties consistent with the
10 letter and intent of the authorization.

11 Id.

12 Attorney General Alberto Gonzales subsequently confirmed
13 that this program intercepts "contents of communications where * * *
14 one party to the communication is outside the United States" and
15 the government has "a reasonable basis to conclude that one party
16 to the communication is a member of al Qaeda, affiliated with al
17 Qaeda, or a member of an organization affiliated with al Qaeda, or
18 working in support of al Qaeda." Doc #87 (AT&T Request for
19 Judicial Notice), Ex J at 1 (hereinafter "12/19/05 Press
20 Briefing"), available at [http://www.whitehouse.gov/news/releases/
21 2005/12/print/20051219-1.html](http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html) (last visited July 19, 2005). The
22 Attorney General also noted, "This [program] is not about
23 wiretapping everyone. This is a very concentrated, very limited
24 program focused at gaining information about our enemy." Id at 5.
25 The President has also made a public statement, of which the court
26 takes judicial notice, that the government's "international
27 activities strictly target al Qaeda and their known affiliates,"
28 "the government does not listen to domestic phone calls without
court approval" and the government is "not mining or trolling
through the personal lives of millions of innocent Americans." The
White House, *President Bush Discusses NSA Surveillance Program* (May
11, 2006) (hereinafter "5/11/06 Statement"), [http://www.whitehouse.](http://www.whitehouse)

1 gov/news/releases/2006/05/20060511-1.html (last visited July 19,
2 2005).

3 On May 11, 2006, USA Today reported the existence of a
4 second NSA program in which BellSouth Corp, Verizon Communications
5 Inc and AT&T were alleged to have provided telephone calling
6 records of tens of millions of Americans to the NSA. Doc #182
7 (Markman Decl), Ex 5 at 1 (Leslie Cauley, *NSA Has Massive Database*
8 *of Americans' Phone Calls*, USA Today (May 11, 2006)). The article
9 did not allege that the NSA listens to or records conversations but
10 rather that BellSouth, Verizon and AT&T gave the government access
11 to a database of domestic communication records that the NSA uses
12 "to analyze calling patterns in an effort to detect terrorist
13 activity." Id. The report indicated a fourth telecommunications
14 company, Qwest Communications International Inc, declined to
15 participate in the program. Id at 2. An attorney for Qwest's
16 former CEO, Joseph Nacchio, issued the following statement:

17 In the Fall of 2001 * * * while Mr Nacchio was
18 Chairman and CEO of Qwest and was serving pursuant
19 to the President's appointment as the Chairman of
20 the National Security Telecommunications Advisory
21 Committee, Qwest was approached to permit the
22 Government access to the private telephone records
23 of Qwest customers.

24 Mr Nacchio made inquiry as to whether a warrant or
25 other legal process had been secured in support of
26 that request. When he learned that no such
27 authority had been granted and that there was a
28 disinclination on the part of the authorities to
use any legal process, including the Special Court
which had been established to handle such matters,
Mr Nacchio concluded that these requests violated
the privacy requirements of the Telecommunications
[sic] Act. Accordingly, Mr Nacchio issued
instructions to refuse to comply with these
requests. These requests continued throughout Mr
Nacchio's tenure and until his departure in June of
2002.

1 Markman Decl, Ex 6.

2 BellSouth and Verizon both issued statements, of which
3 the court takes judicial notice, denying their involvement in the
4 program described in USA Today. BellSouth stated in relevant part:

5 As a result of media reports that BellSouth
6 provided massive amounts of customer calling
7 information under a contract with the NSA, the
8 Company conducted an internal review to determine
9 the facts. Based on our review to date, we have
10 confirmed no such contract exists and we have not
11 provided bulk customer calling records to the NSA.

12 News Release, BellSouth Statement on Governmental Data Collection
13 (May 15, 2006), available at [http://bellsouth.mediaroom.com/](http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860)
14 [index.php?s=press_releases&item=2860](http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860) (last visited July 19, 2006).

15 Although declining to confirm or deny whether it had any
16 relationship to the NSA program acknowledged by the President,
17 Verizon stated in relevant part:

18 One of the most glaring and repeated falsehoods in
19 the media reporting is the assertion that, in the
20 aftermath of the 9/11 attacks, Verizon was
21 approached by NSA and entered into an arrangement
22 to provide the NSA with data from its customers'
23 domestic calls.

24 This is false. From the time of the 9/11 attacks
25 until just four months ago, Verizon had three major
26 businesses - its wireline phone business, its
27 wireless company and its directory publishing
28 business. It also had its own Internet Service
29 Provider and long-distance businesses. Contrary to
30 the media reports, Verizon was not asked by NSA to
31 provide, nor did Verizon provide, customer phone
32 records from any of these businesses, or any call
33 data from those records. None of these companies
34 — wireless or wireline — provided customer
35 records or call data.

36 See News Release, Verizon Issues Statement on NSA Media Coverage
37 (May 16, 2006), available at [http://newscenter.verizon.com/](http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450)
38 [proactive/newsroom/release.vtml?id=93450](http://newscenter.verizon.com/proactive/newsroom/release.vtml?id=93450) (last visited July 19,
2006). BellSouth and Verizon's denials have been at least somewhat

1 substantiated in later reports. Doc #298 (DiMuzio Decl), Ex 1
2 (*Lawmakers: NSA Database Incomplete*, USA Today (June 30, 2006)).
3 Neither AT&T nor the government has confirmed or denied the
4 existence of a program of providing telephone calling records to
5 the NSA. Id.

6
7 2

8 Although the government does not claim that the AT&T
9 documents obtained by Mark Klein or the accompanying declarations
10 contain classified information (Doc #284 (6/23/06 Transcript) at
11 76:9-20), those papers remain under seal because AT&T alleges that
12 they contain proprietary and trade secret information.
13 Nonetheless, much of the information in these papers has already
14 been leaked to the public or has been revealed in redacted versions
15 of the papers. The summary below is based on those already
16 disclosed facts.

17 In a public statement, Klein explained that while working
18 at an AT&T office in San Francisco in 2002, "the site manager told
19 me to expect a visit from a National Security Agency agent, who was
20 to interview a management-level technician for a special job." Doc
21 #43 (Ericson Decl), Ex J at 1. While touring the Folsom Street
22 AT&T facility in January 2003, Klein "saw a new room being built
23 adjacent to the 4ESS switch room where the public's phone calls are
24 routed" and "learned that the person whom the NSA interviewed for
25 the secret job was the person working to install equipment in this
26 room." Id. See also Doc #147 (Redact Klein Decl), ¶ 10 ("The NSA
27 agent came and met with [Field Support Specialist (FSS)] #2. FSS
28 #1 later confirmed to me that FSS #2 was working on the special

1 job."); id, ¶ 16 ("In the Fall of 2003, FSS #1 told me that another
2 NSA agent would again visit our office * * * to talk to FSS #1 in
3 order to get the latter's evaluation of FSS #3's suitability to
4 perform the special job that FSS #2 had been doing. The NSA agent
5 did come and speak to FSS #1.").

6 Klein then learned about the AT&T documents in October
7 2003, after being transferred to the Folsom Street facility to
8 oversee the Worldnet Internet room. Ericson Decl, Ex J at 2. One
9 document described how "fiber optic cables from the secret room
10 were tapping into the Worldnet circuits by splitting off a portion
11 of the light signal." Id. The other two documents "instructed
12 technicians on connecting some of the already in-service circuits
13 to [a] 'splitter' cabinet, which diverts some of the light signal
14 to the secret room." Id. Klein noted the secret room contained "a
15 Narus STA 6400" and that "Narus STA technology is known to be used
16 particularly by government intelligence agencies because of its
17 ability to sift through large amounts of data looking for
18 preprogrammed targets." Id. Klein also "learned that other such
19 'splitter' cabinets were being installed in other cities, including
20 Seattle, San Jose, Los Angeles and San Diego." Id.

21
22 D

23 Based on the foregoing, it might appear that none of the
24 subject matter in this litigation could be considered a secret
25 given that the alleged surveillance programs have been so widely
26 reported in the media.

27 //

28 //

1 The court recognizes, however, that simply because a
2 factual statement has been publicly made does not necessarily mean
3 that the facts it relates are true and are not a secret. The
4 statement also must come from a reliable source. Indeed, given the
5 sheer amount of statements that have been made in the public sphere
6 about the alleged surveillance programs and the limited number of
7 permutations that such programs could take, it would seem likely
8 that the truth about these programs has already been publicly
9 reported somewhere. But simply because such statements have been
10 publicly made does not mean that the truth of those statements is a
11 matter of general public knowledge and that verification of the
12 statement is harmless.

13 In determining whether a factual statement is a secret
14 for purposes of the state secrets privilege, the court should look
15 only at publicly reported information that possesses substantial
16 indicia of reliability and whose verification or substantiation
17 possesses the potential to endanger national security. That
18 entails assessing the value of the information to an individual or
19 group bent on threatening the security of the country, as well as
20 the secrecy of the information.

21 For instance, if this litigation verifies that AT&T
22 assists the government in monitoring communication records, a
23 terrorist might well cease using AT&T and switch to other, less
24 detectable forms of communication. Alternatively, if this
25 litigation reveals that the communication records program does not
26 exist, then a terrorist who had been avoiding AT&T might start
27 using AT&T if it is a more efficient form of communication. In
28 short, when deciding what communications channel to use, a

1 terrorist "balanc[es] the risk that a particular method of
2 communication will be intercepted against the operational
3 inefficiencies of having to use ever more elaborate ways to
4 circumvent what he thinks may be intercepted." 6/23/06 Transcript
5 at 48:14-17 (government attorney). A terrorist who operates with
6 full information is able to communicate more securely and more
7 efficiently than a terrorist who operates in an atmosphere of
8 uncertainty.

9 It is, of course, an open question whether individuals
10 inclined to commit acts threatening the national security engage in
11 such calculations. But the court is hardly in a position to
12 second-guess the government's assertions on this matter or to
13 estimate the risk tolerances of terrorists in making their
14 communications and hence at this point in the litigation eschews
15 the attempt to weigh the value of the information.

16 Accordingly, in determining whether a factual statement
17 is a secret, the court considers only public admissions or denials
18 by the government, AT&T and other telecommunications companies,
19 which are the parties indisputably situated to disclose whether and
20 to what extent the alleged programs exist. In determining what is
21 a secret, the court at present refrains from relying on the
22 declaration of Mark Klein. Although AT&T does not dispute that
23 Klein was a former AT&T technician and he has publicly declared
24 under oath that he observed AT&T assisting the NSA in some capacity
25 and his assertions would appear admissible in connection with the
26 present motions, the inferences Klein draws have been disputed. To
27 accept the Klein declaration at this juncture in connection with
28 the state secrets issue would invite attempts to undermine the

1 privilege by mere assertions of knowledge by an interested party.
2 Needless to say, this does not reflect that the court discounts
3 Klein's credibility, but simply that what is or is not secret
4 depends on what the government and its alleged operative AT&T and
5 other telecommunications providers have either admitted or denied
6 or is beyond reasonable dispute.

7 Likewise, the court does not rely on media reports about
8 the alleged NSA programs because their reliability is unclear. To
9 illustrate, after Verizon and BellSouth denied involvement in the
10 program described in USA Today in which communication records are
11 monitored, USA Today published a subsequent story somewhat backing
12 down from its earlier statements and at least in some measure
13 substantiating these companies' denials. See *supra* I(C)(1).

14 Finally, the court notes in determining whether the
15 privilege applies, the court is not limited to considering strictly
16 admissible evidence. FRE 104(a) ("Preliminary questions concerning
17 * * * the existence of a privilege * * * shall be determined by the
18 court, subject to the provisions of subdivision (b). In making its
19 determination it is not bound by the rules of evidence except those
20 with respect to privileges."). This makes sense: the issue at bar
21 is not proving a question of liability but rather determining
22 whether information that the government contends is a secret is
23 actually a secret. In making this determination, the court may
24 rely upon reliable public evidence that might otherwise be
25 inadmissible at trial because it does not comply with the technical
26 requirements of the rules of evidence.

27 With these considerations in mind, the court at last
28 determines whether the state secrets privilege applies here.

E

1
2 Because this case involves an alleged covert relationship
3 between the government and AT&T, the court first determines whether
4 to apply the categorical bar to suit established by the Supreme
5 Court in Totten v United States, 92 US 105 (1875), acknowledged in
6 United States v Reynolds, 345 US 1 (1953) and Kasza v Browner, 133
7 F3d 1159 (9th Cir 1998), and reaffirmed in Tenet v Doe, 544 US 1
8 (2005). See *id* at 6 (“[A]pplication of the Totten rule of
9 dismissal * * * represents the sort of ‘threshold question’ we have
10 recognized may be resolved before addressing jurisdiction.”). The
11 court then examines the closely related questions whether this
12 action must be presently dismissed because “the very subject matter
13 of the action” is a state secret or because the state secrets
14 privilege necessarily blocks evidence essential to plaintiffs’
15 *prima facie* case or AT&T’s defense. See Kasza, 133 F3d at 1166-67.

1

16
17
18 Although the principles announced in Totten, Tenet,
19 Reynolds and Kasza inform the court’s decision here, those cases
20 are not strictly analogous to the facts at bar.

21 First, the instant plaintiffs were not a party to the
22 alleged covert arrangement at issue here between AT&T and the
23 government. Hence, Totten and Tenet are not on point to the extent
24 they hold that former spies cannot enforce agreements with the
25 government because the parties implicitly agreed that such suits
26 would be barred. The implicit notion in Totten was one of
27 equitable estoppel: one who agrees to conduct covert operations
28 impliedly agrees not to reveal the agreement even if the agreement

1 is breached. But AT&T, the alleged spy, is not the plaintiff here.
2 In this case, plaintiffs made no agreement with the government and
3 are not bound by any implied covenant of secrecy.

4 More importantly, unlike the clandestine spy arrangements
5 in Tenet and Totten, AT&T and the government have for all practical
6 purposes already disclosed that AT&T assists the government in
7 monitoring communication content. As noted earlier, the government
8 has publicly admitted the existence of a "terrorist surveillance
9 program," which the government insists is completely legal. This
10 program operates without warrants and targets "contents of
11 communications where * * * one party to the communication is
12 outside the United States" and the government has "a reasonable
13 basis to conclude that one party to the communication is a member
14 of al Qaeda, affiliated with al Qaeda, or a member of an
15 organization affiliated with al Qaeda, or working in support of al
16 Qaeda." 12/19/05 Press Briefing at 1.

17 Given that the "terrorist surveillance program" tracks
18 "calls into the United States or out of the United States," 5/11/06
19 Statement, it is inconceivable that this program could exist
20 without the acquiescence and cooperation of some telecommunications
21 provider. Although of record here only in plaintiffs' pleading, it
22 is beyond reasonable dispute that "prior to its being acquired by
23 SBC, AT&T Corp was the second largest Internet provider in the
24 country," FAC, ¶ 26, and "AT&T Corp's bundled local and long
25 distance service was available in 46 states, covering more than 73
26 million households," id, ¶ 25. AT&T's assistance would greatly
27 help the government implement this program. See also id, ¶ 27
28 ("The new AT&T Inc constitutes the largest telecommunications

1 provider in the United States and one of the largest in the
2 world."). Considering the ubiquity of AT&T telecommunications
3 services, it is unclear whether this program could even exist
4 without AT&T's acquiescence and cooperation.

5 Moreover, AT&T's history of cooperating with the
6 government on such matters is well known. AT&T has recently
7 disclosed that it "performs various classified contracts, and
8 thousands of its employees hold government security clearances."
9 FAC, ¶ 29. More recently, in response to reports on the alleged
10 NSA programs, AT&T has disclosed in various statements, of which
11 the court takes judicial notice, that it has "an obligation to
12 assist law enforcement and other government agencies responsible
13 for protecting the public welfare, whether it be an individual or
14 the security interests of the entire nation. * * * If and when
15 AT&T is asked to help, we do so strictly within the law and under
16 the most stringent conditions." News Release, AT&T Statement on
17 Privacy and Legal/Security Issues (May 11, 2006) (emphasis added),
18 available at [http://www.sbc.com/gen/press-room?pid=4800&cdvn=news](http://www.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22285)
19 [&newsarticleid=22285](http://www.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=22285). See also Declan McCullagh, CNET News.com,
20 Legal Loophole Emerges in NSA Spy Program (May 19, 2006) ("Mark
21 Bien, a spokesman for AT&T, told CNET News.com on Wednesday:
22 'Without commenting on or confirming the existence of the program,
23 we can say that when the government asks for our help in protecting
24 national security, and the request is within the law, we will
25 provide that assistance.'"), available at [http://news.com.com/](http://news.com.com/Legal+loophole+emerges+in+NSA+spy+program/2100-1028_3-6073600.html)
26 [Legal+loophole+emerges+in+NSA+spy+program/2100-1028_3-6073600.html](http://news.com.com/Legal+loophole+emerges+in+NSA+spy+program/2100-1028_3-6073600.html);
27 Justin Scheck, Plaintiffs Can Keep AT&T Papers in Domestic Spying
28 Case, The Recorder (May 18, 2006) ("Marc Bien, a spokesman for

1 AT&T, said he didn't see a settlement on the horizon. 'When the
2 government asks for our help in protecting American security, and
3 the request is within the law, we provide assistance,' he said."),
4 available at <http://www.law.com/jsp/article.jsp?id=1147856734796>.
5 And AT&T at least presently believes that any such assistance would
6 be legal if AT&T were simply a passive agent of the government or
7 if AT&T received a government certification authorizing the
8 assistance. 6/23/06 Transcript at 15:11-21:19. Hence, it appears
9 AT&T helps the government in classified matters when asked and AT&T
10 at least currently believes, on the facts as alleged in plaintiffs'
11 complaint, its assistance is legal.

12 In sum, the government has disclosed the general contours
13 of the "terrorist surveillance program," which requires the
14 assistance of a telecommunications provider, and AT&T claims that
15 it lawfully and dutifully assists the government in classified
16 matters when asked.

17 A remaining question is whether, in implementing the
18 "terrorist surveillance program," the government ever requested the
19 assistance of AT&T, described in these proceedings as the mother of
20 telecommunications "that in a very literal way goes all the way
21 back to Alexander Graham Bell summoning his assistant Watson into
22 the room." Id at 102:11-13. AT&T's assistance in national
23 security surveillance is hardly the kind of "secret" that the
24 Totten bar and the state secrets privilege were intended to protect
25 or that a potential terrorist would fail to anticipate.

26 //

27 //

28 //

1 The court's conclusion here follows the path set in
2 Halkin v Helms and Ellsberg v Mitchell, the two cases most
3 factually similar to the present. The Halkin and Ellsberg courts
4 did not preclude suit because of a Totten-based implied covenant of
5 silence. Although the courts eventually terminated some or all of
6 plaintiffs' claims because the privilege barred discovery of
7 certain evidence (Halkin I, 598 F2d at 10; Halkin II, 690 F2d at
8 980, 987-88; Ellsberg, 709 F2d at 65), the courts did not dismiss
9 the cases at the outset, as would have been required had the Totten
10 bar applied. Accordingly, the court sees no reason to apply the
11 Totten bar here.

12 For all of the above reasons, the court declines to
13 dismiss this case based on the categorical Totten/Tenet bar.

14
15 2

16 The court must also dismiss this case if "the very
17 subject matter of the action" is a state secret and therefore "any
18 further proceeding * * * would jeopardize national security."
19 Kasza, 133 F3d at 1170. As a preliminary matter, the court agrees
20 that the government has satisfied the three threshold requirements
21 for properly asserting the state secrets privilege: (1) the head
22 of the relevant department, Director of National Intelligence John
23 D Negroponete (2) has lodged a formal claim of privilege (Negroponete
24 Decl, ¶¶ 9, 13) (3) after personally considering the matter (Id, ¶¶
25 2, 9, 13). Moreover, the Director of the NSA, Lieutenant General
26 Keith B Alexander, has filed a declaration supporting Director
27 Negroponete's assertion of the privilege. Alexander Decl, ¶¶ 2, 9.

28 //

1 The court does not "balanc[e the] ultimate interests at
2 stake in the litigation." Halkin II, 690 F2d at 990. But no case
3 dismissed because its "very subject matter" was a state secret
4 involved ongoing, widespread violations of individual
5 constitutional rights, as plaintiffs allege here. Indeed, most
6 cases in which the "very subject matter" was a state secret
7 involved classified details about either a highly technical
8 invention or a covert espionage relationship. See, e g, Sterling v
9 Tenet, 416 F3d 338, 348 (4th Cir 2005) (dismissing Title VII racial
10 discrimination claim that "center[ed] around a covert agent's
11 assignments, evaluations, and colleagues"); Kasza, 133 F3d at 1162-
12 63, 1170 (dismissing RCRA claim regarding facility reporting and
13 inventory requirements at a classified Air Force location near
14 Groom Lake, Nevada); Zuckerbraun v General Dynamics Corp, 935 F2d
15 544, 547-48 (2d Cir 1991) (dismissing wrongful death claim
16 implicating classified information about the "design, manufacture,
17 performance, functional characteristics, and testing of [weapons]
18 systems and the rules of engagement"); Fitzgerald v Penthouse Intl,
19 776 F2d 1236, 1242-43 (4th Cir 1985) (dismissing libel suit
20 "charging the plaintiff with the unauthorized sale of a top secret
21 marine mammal weapons system"); Halpern v United States, 258 F2d
22 36, 44 (2d Cir 1958) (rejecting government's motion to dismiss in a
23 case involving a patent with military applications withheld under a
24 secrecy order); Clift v United States, 808 F Supp 101, 111 (D Conn
25 1991) (dismissing patent dispute over a cryptographic encoding
26 device).

27 //

28 //

1 By contrast, the very subject matter of this action is
2 hardly a secret. As described above, public disclosures by the
3 government and AT&T indicate that AT&T is assisting the government
4 to implement some kind of surveillance program. See *supra* I(E)(1).

5 For this reason, the present action is also different
6 from El-Masri v Tenet, the recently dismissed case challenging the
7 government's alleged "extraordinary rendition program." In El-
8 Masri, only limited sketches of the alleged program had been
9 disclosed and the whole object of the suit was to reveal classified
10 details regarding "the means and methods the foreign intelligence
11 services of this and other countries used to carry out the
12 program." El-Masri, 2006 WL 1391390, *5. By contrast, this case
13 focuses only on whether AT&T intercepted and disclosed
14 communications or communication records to the government. And as
15 described above, significant amounts of information about the
16 government's monitoring of communication content and AT&T's
17 intelligence relationship with the government are already non-
18 classified or in the public record.

19
20 3

21 The court also declines to decide at this time whether
22 this case should be dismissed on the ground that the government's
23 state secrets assertion will preclude evidence necessary for
24 plaintiffs to establish a *prima facie* case or for AT&T to raise a
25 valid defense to the claims. Plaintiffs appear to be entitled to
26 at least some discovery. See *infra* I(G)(3). It would be premature
27 to decide these issues at the present time. In drawing this
28 conclusion, the court is following the approach of the courts in

1 Halkin v Helms and Ellsberg v Mitchell; these courts did not
2 dismiss those cases at the outset but allowed them to proceed to
3 discovery sufficiently to assess the state secrets privilege in
4 light of the facts. The government has not shown why that should
5 not be the course of this litigation.

6
7 4

8 In sum, for much the same reasons that Totten does not
9 preclude this suit, the very subject matter of this action is not a
10 "secret" for purposes of the state secrets privilege and it would
11 be premature to conclude that the privilege will bar evidence
12 necessary for plaintiffs' *prima facie* case or AT&T's defense.
13 Because of the public disclosures by the government and AT&T, the
14 court cannot conclude that merely maintaining this action creates a
15 "reasonable danger" of harming national security. Accordingly,
16 based on the foregoing, the court DENIES the government's motion to
17 dismiss.

18
19 F

20 The court hastens to add that its present ruling should
21 not suggest that its *in camera*, *ex parte* review of the classified
22 documents confirms the truth of the particular allegations in
23 plaintiffs' complaint. Plaintiffs allege a surveillance program of
24 far greater scope than the publicly disclosed "terrorist
25 surveillance program." The existence of this alleged program and
26 AT&T's involvement, if any, remain far from clear. And as in
27 Halkin v Helms, it is certainly possible that AT&T might be
28 entitled to summary judgment at some point if the court finds that

1 the state secrets privilege blocks certain items of evidence that
2 are essential to plaintiffs' *prima facie* case or AT&T's defense.
3 The court also recognizes that legislative or other developments
4 might alter the course of this litigation.

5 But it is important to note that even the state secrets
6 privilege has its limits. While the court recognizes and respects
7 the executive's constitutional duty to protect the nation from
8 threats, the court also takes seriously its constitutional duty to
9 adjudicate the disputes that come before it. See Hamdi v Rumsfeld,
10 542 US 507, 536 (2004) (plurality opinion) ("Whatever power the
11 United States Constitution envisions for the Executive in its
12 exchanges with other nations or with enemy organizations in times
13 of conflict, it most assuredly envisions a role for all three
14 branches when individual liberties are at stake."). To defer to a
15 blanket assertion of secrecy here would be to abdicate that duty,
16 particularly because the very subject matter of this litigation has
17 been so publicly aired. The compromise between liberty and
18 security remains a difficult one. But dismissing this case at the
19 outset would sacrifice liberty for no apparent enhancement of
20 security.

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

G

The government also contends the issue whether AT&T received a certification authorizing its assistance to the government is a state secret. Gov 5/17/06 Br at 17.

1

The procedural requirements and impact of a certification under Title III are addressed in 18 USC § 2511(2) (a) (ii):

Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, * * * are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of [FISA] * * * if such provider, its officers, employees, or agents, * * * has been provided with — * * *

(B) a certification in writing by a person specified in section 2518(7) of this title [18 USCS § 2518(7)] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required * * *.

Although it is doubtful whether plaintiffs' constitutional claim would be barred by a valid certification under section 2511(2) (a) (ii), this provision on its face makes clear that a valid certification would preclude the statutory claims asserted here. See 18 USC § 2511(2) (a) (ii) ("No cause of action shall lie in any court against any provider of wire or electronic communication service * * * for providing information, facilities, or assistance in accordance with the terms of a * * * certification under this chapter.").

//

As noted above, it is not a secret for purposes of the state secrets privilege that AT&T and the government have some kind of intelligence relationship. See *supra* I(E)(1). Nonetheless, the court recognizes that uncovering whether and to what extent a certification exists might reveal information about AT&T's assistance to the government that has not been publicly disclosed. Accordingly, in applying the state secrets privilege to the certification question, the court must look deeper at what information has been publicly revealed about the alleged electronic surveillance programs. The following chart summarizes what the government has disclosed about the scope of these programs in terms of (1) the individuals whose communications are being monitored, (2) the locations of those individuals and (3) the types of information being monitored:

	Purely domestic communication content	Domestic-foreign communication content	Communication records
General public	Government DENIES	Government DENIES	Government NEITHER CONFIRMS NOR DENIES
al Qaeda or affiliate member/agent	Government DENIES	Government CONFIRMS	

As the chart relates, the government's public disclosures regarding monitoring of "communication content" (i e, wiretapping or listening in on a communication) differ significantly from its disclosures regarding "communication records" (i e, collecting ancillary data pertaining to a communication, such as the telephone

1 numbers dialed by an individual). See *supra* I(C)(1). Accordingly,
2 the court separately addresses for each alleged program whether
3 revealing the existence or scope of a certification would disclose
4 a state secret.

5
6 3

7 Beginning with the warrantless monitoring of
8 "communication content," the government has confirmed that it
9 monitors "contents of communications where * * * one party to the
10 communication is outside the United States" and the government has
11 "a reasonable basis to conclude that one party to the communication
12 is a member of al Qaeda, affiliated with al Qaeda, or a member of
13 an organization affiliated with al Qaeda, or working in support of
14 al Qaeda." 12/19/05 Press Briefing at 1. The government denies
15 listening in without a warrant on any purely domestic
16 communications or communications in which neither party has a
17 connection to al Qaeda or a related terrorist organization. In
18 sum, regarding the government's monitoring of "communication
19 content," the government has disclosed the universe of
20 possibilities in terms of whose communications it monitors and
21 where those communicating parties are located.

22 Based on these public disclosures, the court cannot
23 conclude that the existence of a certification regarding the
24 "communication content" program is a state secret. If the
25 government's public disclosures have been truthful, revealing
26 whether AT&T has received a certification to assist in monitoring
27 communication content should not reveal any new information that
28 would assist a terrorist and adversely affect national security.

1 And if the government has not been truthful, the state secrets
2 privilege should not serve as a shield for its false public
3 statements. In short, the government has opened the door for
4 judicial inquiry by publicly confirming and denying material
5 information about its monitoring of communication content.

6 Accordingly, the court concludes that the state secrets
7 privilege will not prevent AT&T from asserting a certification-
8 based defense, as appropriate, regarding allegations that it
9 assisted the government in monitoring communication content. The
10 court envisions that AT&T could confirm or deny the existence of a
11 certification authorizing monitoring of communication content
12 through a combination of responses to interrogatories and *in camera*
13 review by the court. Under this approach, AT&T could reveal
14 information at the level of generality at which the government has
15 publicly confirmed or denied its monitoring of communication
16 content. This approach would also enable AT&T to disclose the non-
17 privileged information described here while withholding any
18 incidental privileged information that a certification might
19 contain.

20
21 4

22 Turning to the alleged monitoring of communication
23 records, the court notes that despite many public reports on the
24 matter, the government has neither confirmed nor denied whether it
25 monitors communication records and has never publicly disclosed
26 whether the NSA program reported by USA Today on May 11, 2006,
27 actually exists. Although BellSouth, Verizon and Qwest have denied
28 participating in this program, AT&T has neither confirmed nor

1 denied its involvement. Hence, unlike the program monitoring
2 communication content, the general contours and even the existence
3 of the alleged communication records program remain unclear.

4 Nonetheless, the court is hesitant to conclude that the
5 existence or non-existence of the communication records program
6 necessarily constitutes a state secret. Confirming or denying the
7 existence of this program would only affect a terrorist who was
8 insensitive to the publicly disclosed "terrorist surveillance
9 program" but cared about the alleged program here. This would seem
10 unlikely to occur in practice given that the alleged communication
11 records program, which does not involve listening in on
12 communications, seems less intrusive than the "terrorist
13 surveillance program," which involves wiretapping. And in any
14 event, it seems odd that a terrorist would continue using AT&T
15 given that BellSouth, Verizon and Qwest have publicly denied
16 participating in the alleged communication records program and
17 would appear to be safer choices. Importantly, the public denials
18 by these telecommunications companies undercut the government and
19 AT&T's contention that revealing AT&T's involvement or lack thereof
20 in the program would disclose a state secret.

21 Still, the court recognizes that it is not in a position
22 to estimate a terrorist's risk preferences, which might depend on
23 facts not before the court. For example, it may be that a
24 terrorist is unable to avoid AT&T by choosing another provider or,
25 for reasons outside his control, his communications might
26 necessarily be routed through an AT&T facility. Revealing that a
27 communication records program exists might encourage that terrorist
28 to switch to less efficient but less detectable forms of

1 communication. And revealing that such a program does not exist
2 might encourage a terrorist to use AT&T services when he would not
3 have done so otherwise. Accordingly, for present purposes, the
4 court does not require AT&T to disclose what relationship, if any,
5 it has with this alleged program.

6 The court stresses that it does not presently conclude
7 that the state secrets privilege will necessarily preclude AT&T
8 from revealing later in this litigation information about the
9 alleged communication records program. While this case has been
10 pending, the government and telecommunications companies have made
11 substantial public disclosures on the alleged NSA programs. It is
12 conceivable that these entities might disclose, either deliberately
13 or accidentally, other pertinent information about the
14 communication records program as this litigation proceeds. The
15 court recognizes such disclosures might make this program's
16 existence or non-existence no longer a secret. Accordingly, while
17 the court presently declines to permit any discovery regarding the
18 alleged communication records program, if appropriate, plaintiffs
19 can request that the court revisit this issue in the future.

20
21 5

22 Finally, the court notes plaintiffs contend that
23 Congress, through various statutes, has limited the state secrets
24 privilege in the context of electronic surveillance and has
25 abrogated the privilege regarding the existence of a government
26 certification. See Doc #192 (Pl Opp Gov MTD) at 16-26, 45-48.
27 Because these arguments potentially implicate highly complicated
28 separation of powers issues regarding Congress' ability to abrogate

1 what the government contends is a constitutionally protected
2 privilege, the court declines to address these issues presently,
3 particularly because the issues might very well be obviated by
4 future public disclosures by the government and AT&T. If
5 necessary, the court may revisit these arguments at a later stage
6 of this litigation.

7
8 H

9 The government also asserts two statutory privileges in
10 its motion to dismiss that it contends apply "to any intelligence-
11 related information, sources and methods implicated by
12 [p]laintiffs' claims and the information covered by these privilege
13 claims are at least co-extensive with the assertion of the state
14 secrets privilege by the DNI." Gov MTD at 14. First, the
15 government relies on 50 USC § 402 note, which provides:

16 [N]othing in this Act or any other law * * * shall
17 be construed to require the disclosure of the
18 organization or any function of the National
19 Security Agency, of any information with respect to
the activities thereof, or of the names, titles,
salaries, or number of the persons employed by such
agency.

20 The government also relies on 50 USC § 403-1(i)(1), which states,
21 "The Director of National Intelligence shall protect intelligence
22 sources and methods from unauthorized disclosure."

23 Neither of these provisions by their terms requires the
24 court to dismiss this action and it would be premature for the
25 court to do so at this time. In opposing a subsequent summary
26 judgment motion, plaintiffs could rely on many non-classified
27 materials including present and future public disclosures of the
28 government or AT&T on the alleged NSA programs, the AT&T documents

1 and the supporting Klein and Marcus declarations and information
2 gathered during discovery. Hence, it is at least conceivable that
3 some of plaintiffs' claims, particularly with respect to
4 declaratory and injunctive relief, could survive summary judgment.
5 After discovery begins, the court will determine step-by-step
6 whether the privileges prevent plaintiffs from discovering
7 particular evidence. But the mere existence of these privileges
8 does not justify dismissing this case now.

9 Additionally, neither of these provisions block AT&T from
10 producing any certification that it received to assist the
11 government in monitoring communication content, see *supra* I(G)(3).
12 Because information about this certification would be revealed only
13 at the same level of generality as the government's public
14 disclosures, permitting this discovery should not reveal any new
15 information on the NSA's activities or its intelligence sources or
16 methods, assuming that the government has been truthful.

17 Accordingly, the court DENIES the government's motion to
18 dismiss based on the statutory privileges and DENIES the privileges
19 with respect to any certification that AT&T might have received
20 authorizing it to monitor communication content.

21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

II

AT&T moves to dismiss plaintiffs' complaint on multiple grounds, contending that (1) plaintiffs lack standing, (2) the amended complaint fails to plead affirmatively the absence of immunity from suit and (3) AT&T is entitled to statutory, common law and qualified immunity. Because standing is a threshold jurisdictional question, the court addresses that issue first. See Steel Company v Citizens for a Better Environment, 523 US 83, 94, 102 (1998).

A

"[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III." Lujan v Defenders of Wildlife, 504 US 555, 560 (1992). To establish standing under Article III, a plaintiff must satisfy three elements: (1) "the plaintiff must have suffered an injury in fact — an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical," (2) "there must be a causal connection between the injury and the conduct complained of" and (3) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id* at 560-61 (internal quotation marks, citations and footnote omitted). A party invoking federal jurisdiction has the burden of establishing its standing to sue. *Id* at 561.

//
//
//

1 In the present case, AT&T contends plaintiffs have not
2 sufficiently alleged injury-in-fact and their complaint relies on
3 "wholly conclusory" allegations. AT&T MTD at 20-22. According to
4 AT&T, "Absent some concrete allegation that the government
5 monitored their communications or records, all plaintiffs really
6 have is a suggestion that AT&T provided a means by which the
7 government could have done so had it wished. This is anything but
8 injury-in-fact." Id at 20 (emphasis in original). AT&T compares
9 this case to United Presbyterian Church v Reagan, 738 F2d 1375 (DC
10 Cir 1984) (written by then-Judge Scalia), in which the court found
11 that plaintiffs' allegations of unlawful surveillance were "too
12 generalized and nonspecific to support a complaint." Id at 1380.

13 As a preliminary matter, AT&T incorrectly focuses on
14 whether plaintiffs have pled that the government "monitored
15 [plaintiffs'] communications or records" or "targeted [plaintiffs]
16 or their communications." Instead, the proper focus is on AT&T's
17 actions. Plaintiffs' statutory claims stem from injuries caused
18 solely by AT&T through its alleged interception, disclosure, use,
19 divulgence and/or publication of plaintiffs' communications or
20 communication records. FAC, ¶¶ 93-95, 102-05, 113-14, 121, 128,
21 135-41. Hence, plaintiffs need not allege any facts regarding the
22 government's conduct to state these claims.

23 More importantly, for purposes of the present motion to
24 dismiss, plaintiffs have stated sufficient facts to allege injury-
25 in-fact for all their claims. "At the pleading stage, general
26 factual allegations of injury resulting from the defendant's
27 conduct may suffice, for on a motion to dismiss we 'presume that
28 general allegations embrace those specific facts that are necessary

1 to support the claim.'" Lujan, 504 US at 561 (quoting Lujan v
2 National Wildlife Federation, 497 US 871, 889 (1990)). Throughout
3 the complaint, plaintiffs generally describe the injuries they have
4 allegedly suffered because of AT&T's illegal conduct and its
5 collaboration with the government. See, e g, FAC, ¶ 61 ("On
6 information and belief, AT&T Corp has provided the government with
7 direct access to the contents of the Hawkeye, Aurora and/or other
8 databases that it manages using Daytona, including all information,
9 records, [dialing, routing, addressing and/or signaling
10 information] and [customer proprietary network information]
11 pertaining to [p]laintiffs and class members, by providing the
12 government with copies of the information in the databases and/or
13 by giving the government access to Daytona's querying capabilities
14 and/or some other technology enabling the government agents to
15 search the databases' contents."); id, ¶ 6 ("On information and
16 belief, AT&T Corp has opened its key telecommunications facilities
17 and databases to direct access by the NSA and/or other government
18 agencies, intercepting and disclosing to the government the
19 contents of its customers' communications as well as detailed
20 communications records about millions of its customers, including
21 [p]laintiffs and class members.").

22 By contrast, plaintiffs in United Presbyterian Church
23 alleged they "ha[d] been informed on numerous occasions" that mail
24 that they had sent never reached its destination, "ha[d] reason to
25 believe that, for a long time, [their] officers, employees, and
26 persons associated with [them had] been subjected to government
27 surveillance, infiltration and disruption" and "discern[ed] a long-
28 term pattern of surveillance of [their] members, disruption of

1 their speaking engagements in this country, and attempts at
2 character assassination." See 738 F2d at 1380 n2. Because these
3 allegations were more attenuated and less concrete than the
4 specific injuries alleged here, United Presbyterian Church does not
5 support dismissing this action.

6 AT&T also contends "[p]laintiffs lack standing to assert
7 their statutory claims (Counts II-VII) because the FAC alleges no
8 facts suggesting that their statutory rights have been violated"
9 and "the FAC alleges nothing to suggest that the named plaintiffs
10 were themselves subject to surveillance." AT&T MTD at 24-25
11 (emphasis in original). But AT&T ignores that the gravamen of
12 plaintiffs' complaint is that AT&T has created a dragnet that
13 collects the content and records of its customers' communications.
14 See, e g, FAC, ¶¶ 42-64. The court cannot see how any one
15 plaintiff will have failed to demonstrate injury-in-fact if that
16 plaintiff effectively demonstrates that all class members have so
17 suffered. This case is plainly distinguishable from Halkin II, for
18 in that case, showing that plaintiffs were on a watchlist was not
19 tantamount to showing that any particular plaintiff suffered a
20 surveillance-related injury-in-fact. See Halkin II, 690 F2d at
21 999-1001. As long as the named plaintiffs were, as they allege,
22 AT&T customers during the relevant time period (FAC, ¶¶ 13-16), the
23 alleged dragnet would have imparted a concrete injury on each of
24 them.

25 //

26 //

27 //

28 //

1 This conclusion is not altered simply because the alleged
2 injury is widely shared among AT&T customers. In FEC v Akins, 524
3 US 11 (1998), the Supreme Court explained:

4 Whether styled as a constitutional or prudential
5 limit on standing, the Court has sometimes
6 determined that where large numbers of Americans
7 suffer alike, the political process, rather than
8 the judicial process, may provide the more
9 appropriate remedy for a widely shared grievance.

10 [This] kind of judicial language * * * however,
11 invariably appears in cases where the harm at issue
12 is not only widely shared, but is also of an
13 abstract and indefinite nature.

14 Id at 23. The Court continued:

15 [W]here a harm is concrete, though widely shared,
16 the Court has found "injury in fact." Thus the
17 fact that a political forum may be more readily
18 available where an injury is widely shared (while
19 counseling against, say, interpreting a statute as
20 conferring standing) does not, by itself,
21 automatically disqualify an interest for Article
22 III purposes. Such an interest, where sufficiently
23 concrete, may count as an "injury in fact."

24 Id at 24.

25 Here, the alleged injury is concrete even though it is
26 widely shared. Despite AT&T's alleged creation of a dragnet to
27 intercept all or substantially all of its customers'
28 communications, this dragnet necessarily inflicts a concrete injury
that affects each customer in a distinct way, depending on the
content of that customer's communications and the time that
customer spends using AT&T services. Indeed, the present situation
resembles a scenario in which "large numbers of individuals suffer
the same common-law injury (say, a widespread mass tort)." Id.

//

//

//

1 AT&T also contends that the state secrets privilege bars
2 plaintiffs from establishing standing. Doc #244 (AT&T Reply) at
3 16-18. See also Gov MTD 16-20. But as described above, the state
4 secrets privilege will not prevent plaintiffs from receiving at
5 least some evidence tending to establish the factual predicate for
6 the injury-in-fact underlying their claims directed at AT&T's
7 alleged involvement in the monitoring of communication content.
8 See *supra* I(G) (3). And the court recognizes that additional facts
9 might very well be revealed during, but not as a direct consequence
10 of, this litigation that obviate many of the secrecy concerns
11 currently at issue regarding the alleged communication records
12 program. Hence, it is unclear whether the privilege would
13 necessarily block AT&T from revealing information about its
14 participation, if any, in that alleged program. See *supra* I(G) (4).
15 The court further notes that the AT&T documents and the
16 accompanying Klein and Marcus declarations provide at least some
17 factual basis for plaintiffs' standing. Accordingly, the court
18 does not conclude at this juncture that plaintiffs' claims would
19 necessarily lack the factual support required to withstand a future
20 jurisdictional challenge based on lack of standing.

21 Because plaintiffs have sufficiently alleged that they
22 suffered an actual, concrete injury traceable to AT&T and
23 redressable by this court, the court DENIES AT&T's motion to
24 dismiss for lack of standing.

25 //

26 //

27 //

28 //

1 B

2 AT&T also contends that telecommunications providers are
3 immune from suit if they receive a government certification
4 authorizing them to conduct electronic surveillance. AT&T MTD at
5 5. AT&T argues that plaintiffs have the burden to plead
6 affirmatively that AT&T lacks such a certification and that
7 plaintiffs have failed to do so here, thereby making dismissal
8 appropriate. Id at 10-13.

9 As discussed above, the procedural requirements for a
10 certification are addressed in 18 USC § 2511(2)(a)(ii)(B). See
11 supra I(G)(1). Under section 2511(2)(a)(ii), "No cause of action
12 shall lie in any court against any provider of wire or electronic
13 communication service * * * for providing information, facilities,
14 or assistance in accordance with the terms of a * * * certification
15 under this chapter." This provision is referenced in 18 USC §
16 2520(a) (emphasis added), which creates a private right of action
17 under Title III:

18 Except as provided in section 2511(2)(a)(ii), any
19 person whose wire, oral, or electronic
20 communication is intercepted, disclosed, or
21 intentionally used in violation of this chapter [18
22 USCS §§ 2510 et seq] may in a civil action recover
23 from the person or entity, other than the United
24 States, which engaged in that violation such relief
25 as may be appropriate.

26 A similar provision exists at 18 USC § 2703(e) (emphasis added):

27 No cause of action shall lie in any court against
28 any provider of wire or electronic communication
service, its officers, employees, agents, or other
specified persons for providing information,
facilities, or assistance in accordance with the
terms of a court order, warrant, subpoena,
statutory authorization, or certification under
this chapter.

1 The court recognizes that the language emphasized above
2 suggests that to state a claim under these statutes, a plaintiff
3 must affirmatively allege that a telecommunications provider did
4 not receive a government certification. And out of the many
5 statutory exceptions in section 2511, only section 2511(2)(a)(ii)
6 appears in section 2520(a), thereby suggesting that a lack of
7 certification is an element of a Title III claim whereas the other
8 exceptions are simply affirmative defenses. As AT&T notes, this
9 interpretation is at least somewhat supported by the Senate report
10 accompanying 18 USC § 2520, which states in relevant part:

11 A civil action will not lie [under 18 USC § 2520]
12 where the requirements of sections 2511(2)(a)(ii) of
13 title 18 are met. With regard to that exception,
the Committee intends that the following procedural
standards will apply:

14 (1) The complaint must allege that a wire or
15 electronic communications service provider (or
one of its employees) (a) disclosed the
16 existence of a wiretap; (b) acted without a
facially valid court order or certification;
17 (c) acted beyond the scope of a court order or
certification or (d) acted on bad faith.
18 Acting in bad faith would include failing to
read the order or collusion. If the complaint
19 fails to make any of these allegations, the
defendant can move to dismiss the complaint for
20 failure to state a claim upon which relief can
be granted.

21 ECPA, S Rep No 99-541, 99th Cong, 2d Sess 26 (1986) (reprinted in
22 1986 USCCAN 3555, 3580) (emphasis added).

23 Nonetheless, the statutory text does not explicitly
24 provide for a heightened pleading requirement, which is in essence
25 what AT&T seeks to impose here. And the court is reluctant to
26 infer a heightened pleading requirement into the statute given that
27 in other contexts, Congress has been explicit when it intended to
28 create such a requirement. See, e g, Private Securities Litigation

1 Reform Act of 1995, § 101, 15 USC § 78u-4(b) (1), (2) (prescribing
2 heightened pleading standards for securities class actions).

3 In any event, the court need not decide whether
4 plaintiffs must plead affirmatively the absence of a certification
5 because the present complaint, liberally construed, alleges that
6 AT&T acted outside the scope of any government certification it
7 might have received. In particular, paragraphs 81 and 82, which
8 are incorporated in all of plaintiffs' claims, state:

9 81. On information and belief, the
10 above-described acts [by defendants] of
11 interception, disclosure, divulgence and/or use of
12 Plaintiffs' and class members' communications,
13 contents of communications, and records pertaining
14 to their communications occurred without judicial
15 or other lawful authorization, probable cause,
16 and/or individualized suspicion.

17 82. On information and belief, at all
18 relevant times, the government instigated, directed
19 and/or tacitly approved all of the above-described
20 acts of AT&T Corp.

21 FAC, ¶¶ 81-82 (emphasis added).

22 Plaintiffs contend that the phrase "occurred without
23 judicial or other lawful authorization" means that AT&T acted
24 without a warrant or a certification. Doc #176 (Pl Opp AT&T MTD)
25 at 13-15. At oral argument, AT&T took issue with this
26 characterization of "lawful authorization":

27 The emphasis there is on the word 'lawful[.]' When
28 you read that paragraph in context, it's clear that
what [plaintiffs are] saying is that any
authorization [AT&T] receive[s] is, in
[plaintiffs'] view, unlawful. And you can see that
because of the other paragraphs in the complaint.
The very next one, [p]aragraph 82, is the paragraph
where [plaintiffs] allege that the United States
government approved and instigated all of our
actions. It wouldn't be reasonable to construe
Paragraph 81 as saying that [AT&T was] not
authorized by the government to do what [AT&T]
allegedly did when the very next paragraph states
the exact opposite.

1 6/23/06 Transcript at 10:21-11:6. Indeed, the court does not
2 question that it would be extraordinary for a large, sophisticated
3 entity like AT&T to assist the government in a warrantless
4 surveillance program without receiving a certification to insulate
5 its actions.

6 Nonetheless, paragraph 81 could be reasonably interpreted
7 as alleging just that. Even if "the government instigated,
8 directed and/or tacitly approved" AT&T's alleged actions, it does
9 not inexorably follow that AT&T received an official certification
10 blessing its actions. At the hearing, plaintiffs' counsel
11 suggested that they had "information and belief based on the news
12 reports that [the alleged activity] was done based on oral
13 requests" not a written certification. Id at 24:21-22.
14 Additionally, the phrase "judicial or other lawful authorization"
15 in paragraph 81 parallels how "a court order" and "a certification"
16 appear in 18 USC §§ 2511(2)(a)(ii)(A) and (B), respectively; this
17 suggests that "lawful authorization" refers to a certification.
18 Interpreted in this manner, plaintiffs are making a factual
19 allegation that AT&T did not receive a certification.

20 In sum, even if plaintiffs were required to plead
21 affirmatively that AT&T did not receive a certification authorizing
22 its alleged actions, plaintiffs' complaint can fairly be
23 interpreted as alleging just that. Whether and to what extent the
24 government authorized AT&T's alleged conduct remain issues for
25 further litigation. For now, however, the court DENIES AT&T's
26 motion to dismiss on this ground.

27 //

28 //

C

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

AT&T also contends that the complaint should be dismissed because it failed to plead the absence of an absolute common law immunity to which AT&T claims to be entitled. AT&T MTD at 13-15. AT&T asserts that this immunity "grew out of a recognition that telecommunications carriers should not be subject to civil liability for cooperating with government officials conducting surveillance activities. That is true whether or not the surveillance was lawful, so long as the government officials requesting cooperation assured the carrier that it was." Id at 13. AT&T also argues that the statutory immunities do not evince a "congressional purpose to displace, rather than supplement, the common law." Id.

AT&T overstates the case law when intimating that the immunity is long established and unequivocal. AT&T relies primarily on two cases: Halperin v Kissinger, 424 F Supp 838 (DC 1976), revd on other grounds, 606 F2d 1192 (DC Cir 1979) and Smith v Nixon, 606 F2d 1183 (DC Cir 1979). In Halperin, plaintiffs alleged that the Chesapeake and Potomac Telephone Company (C&P) assisted federal officials in illegally wiretapping plaintiffs' home telephone, thereby violating plaintiffs' constitutional and Title III statutory rights. 424 F Supp at 840. In granting summary judgment for C&P, the district court noted:

//
//
//
//
//

1 Chesapeake and Potomac Telephone Company, argues
2 persuasively that it played no part in selecting
3 any wiretap suspects or in determining the length
4 of time the surveillance should remain. It
5 overheard none of plaintiffs' conversations and was
6 not informed of the nature or outcome of the
7 investigation. As in the past, C&P acted in
8 reliance upon a request from the highest Executive
9 officials and with assurances that the wiretap
10 involved national security matters. Under these
11 circumstances, C&P's limited technical role in the
12 surveillance as well as its reasonable expectation
13 of legality cannot give rise to liability for any
14 statutory or constitutional violation.

15 Id at 846.

16 Smith v Nixon involved an allegedly illegal wiretap that
17 was part of the same surveillance program implicated in Halperin.

18 In addressing C&P's potential liability, the Smith court noted:

19 The District Court dismissed the action against
20 C&P, which installed the wiretap, on the ground
21 cited in the District Court's opinion in Halperin:
22 'C&P's limited technical role in the surveillance
23 as well as its reasonable expectation of legality
24 cannot give rise to liability for any statutory or
25 constitutional violation. * * *.' We think this
26 was the proper disposition. The telephone company
27 did not initiate the surveillance, and it was
28 assured by the highest Executive officials in this
nation that the action was legal.

606 F2d at 1191 (citation and footnote omitted) (omission in
original).

The court first observes that Halperin, which formed the
basis for the Smith decision, never indicated that C&P was "immune"
from suit; rather, the court granted summary judgment after it
determined that C&P played only a "limited technical role" in the
surveillance. And although C&P was dismissed in Smith on a motion
to dismiss, Smith never stated that C&P was immune from suit; the
only discussion of "immunity" there related to other defendants who
claimed entitlement to qualified and absolute immunity.

1 At best, the language in Halperin and Smith is equivocal:
2 the phrase "C&P's limited technical role in the surveillance as
3 well as its reasonable expectation of legality cannot give rise to
4 liability for any statutory or constitutional violation" could
5 plausibly be interpreted as describing a good faith defense. And
6 at least one court appears to have interpreted Smith in that
7 manner. See Manufacturas Intl, Ltda v Manufacturers Hanover Trust
8 Co, 792 F Supp 180, 192-93 (EDNY 1992) (referring to Smith while
9 discussing good faith defenses).

10 Moreover, it is not clear at this point in the litigation
11 whether AT&T played a "mere technical role" in the alleged NSA
12 surveillance programs. The complaint alleges that "at all relevant
13 times, the government instigated, directed and/or tacitly approved
14 all of the above-described acts of AT&T Corp." FAC, ¶ 82. But
15 given the massive scale of the programs alleged here and AT&T's
16 longstanding history of assisting the government in classified
17 matters, one could reasonably infer that AT&T's assistance here is
18 necessarily more comprehensive than C&P's assistance in Halperin
19 and Smith. Indeed, there is a world of difference between a single
20 wiretap and an alleged dragnet that sweeps in the communication
21 content and records of all or substantially all AT&T customers.

22 AT&T also relies on two Johnson-era cases: Fowler v
23 Southern Bell Telephone & Telegraph Co, 343 F2d 150 (5th Cir 1965),
24 and Craska v New York Telephone Co, 239 F Supp 932 (NDNY 1965).
25 Fowler involved a Georgia state claim for invasion of right of
26 privacy against a telephone company for assisting federal officers
27 to intercept plaintiff's telephone conversations. Fowler noted
28 that a "defense of privilege" would extend to the telephone company

1 only if the court determined that the federal officers acted within
2 the scope of their duties:

3 If it is established that [the federal officers]
4 acted in the performance and scope of their
5 official powers and within the outer perimeter of
6 their duties as federal officers, then the defense
7 of privilege would be established as to them. In
8 this event the privilege may be extended to
9 exonerate the Telephone Company also if it appears,
10 in line with the allegations of the complaint, that
11 the Telephone Company acted for and at the request
12 of the federal officers and within the bounds of
13 activity which would be privileged as to the
14 federal officers.

15 343 F2d at 156-57 (emphasis added). Accordingly, Fowler does not
16 absolve AT&T of any liability unless and until the court determines
17 that the government acted legally in creating the NSA surveillance
18 programs alleged in the complaint.

19 Craska also does not help AT&T. In that case, plaintiff
20 sued a telephone company for violating her statutory rights by
21 turning over telephone records to the government under compulsion
22 of state law. Craska, 239 F Supp at 933-34, 936. The court
23 declined to ascribe any liability to the telephone company because
24 its assistance was required under state law: "[T]he conduct of the
25 telephone company, acting under the compulsion of State law and
26 process, cannot sensibly be said to have joined in a knowing
27 venture of interception and divulgence of a telephone conversation,
28 which it sought by affirmative action to make succeed." Id at 936.
By contrast, it is not evident whether AT&T was required to help
the government here; indeed, AT&T appears to have confirmed that it
did not have any legal obligation to assist the government
implement any surveillance program. 6/23/06 Transcript at 17:25-
18:4 ("The Court: Well, AT&T could refuse, could it not, to

1 provide access to its facilities? [AT&T]: Yes, it could. Under
2 [18 USC §] 2511, your Honor, AT&T would have the discretion to
3 refuse, and certainly if it believed anything illegal was
4 occurring, it would do so.”).

5 Moreover, even if a common law immunity existed decades
6 ago, applying it presently would undermine the carefully crafted
7 scheme of claims and defenses that Congress established in
8 subsequently enacted statutes. For example, all of the cases cited
9 by AT&T as applying the common law “immunity” were filed before the
10 certification provision of FISA went into effect. See § 301 of
11 FISA. That provision protects a telecommunications provider from
12 suit if it obtains from the Attorney General or other authorized
13 government official a written certification “that no warrant or
14 court order is required by law, that all statutory requirements
15 have been met, and that the specified assistance is required.” 18
16 USC § 2511(2)(a)(ii)(B). Because the common law “immunity” appears
17 to overlap considerably with the protections afforded under the
18 certification provision, the court would in essence be nullifying
19 the procedural requirements of that statutory provision by applying
20 the common law “immunity” here. And given the shallow doctrinal
21 roots of immunity for communications carriers at the time Congress
22 enacted the statutes in play here, there is simply no reason to
23 presume that a common law immunity is available simply because
24 Congress has not expressed a contrary intent. Cf Owen v City of
25 Independence, 445 US 622, 638 (1980) (“[N]otwithstanding § 1983’s
26 expansive language and the absence of any express incorporation of
27 common-law immunities, we have, on several occasions, found that a
28 tradition of immunity was so firmly rooted in the common law and

1 was supported such strong policy reasons that 'Congress would have
2 specifically so provided had it wished to abolish the doctrine.'"
3 (quoting Pierson v Ray, 386 US 547, 555 (1967))).

4 Accordingly, the court DENIES AT&T's motion to dismiss on
5 the basis of a purported common law immunity.

6
7 D

8 AT&T also argues that it is entitled to qualified
9 immunity. AT&T MTD at 16. Qualified immunity shields state actors
10 from liability for civil damages "insofar as their conduct does not
11 violate clearly established statutory or constitutional rights of
12 which a reasonable person would have known." Harlow v Fitzgerald,
13 457 US 800, 818 (1982). "Qualified immunity strikes a balance
14 between compensating those who have been injured by official
15 conduct and protecting government's ability to perform its
16 traditional functions." Wyatt v Cole, 504 US 158, 167 (1992).
17 "[T]he qualified immunity recognized in Harlow acts to safeguard
18 government, and thereby to protect the public at large, not to
19 benefit its agents." Wyatt v Cole, 504 US 158, 168 (1992).
20 Compare AT&T MTD at 17 ("It would make little sense to protect the
21 principal but not its agent."). The Supreme Court does not "draw a
22 distinction for purposes of immunity law between suits brought
23 against state officials under [42 USC] § 1983 and suits brought
24 directly under the Constitution [via Bivens v Six Unknown Named
25 Agents, 403 US 388 (1971)] against federal officials." Butz v
26 Economou, 438 US 478, 504 (1978).

27 //

28 //

1 At the pleadings stage, qualified immunity analysis
2 entails three steps. First, the court must determine whether,
3 taken in the light most favorable to the plaintiff, the facts
4 alleged show a violation of the plaintiffs' statutory or
5 constitutional rights. Saucier v Katz, 533 US 194, 201 (2001). If
6 a violation has been alleged, the court next determines whether the
7 right infringed was clearly established at the time of the alleged
8 violation. Finally, the court assesses whether it would be clear
9 to a reasonable person in the defendant's position that its conduct
10 was unlawful in the situation it confronted. *Id* at 202, 205. See
11 also Frederick v Morse, 439 F3d 1114, 1123 (9th Cir 2006)
12 (characterizing this final inquiry as a discrete third step in the
13 analysis). "This is not to say that an official action is
14 protected by qualified immunity unless the very action in question
15 has previously been held unlawful, but it is to say that in the
16 light of pre-existing law the unlawfulness must be apparent." Hope
17 v Pelzer, 536 US 730, 739 (2002) (citation omitted).

18
19 1

20 When a private party seeks to invoke qualified immunity,
21 the court must first decide whether qualified immunity is
22 "categorically available," which "requires an evaluation of the
23 appropriateness of qualified immunity given its historical
24 availability and the policy considerations underpinning the
25 doctrine." Jensen v Lane County, 222 F3d 570, 576 (9th Cir 2000).
26 This inquiry is distinct from the question whether a nominally
27 private party is a state actor for purposes of a section 1983 or
28 Bivens claim.

1 In Wyatt v Cole, 504 US 158 (1992), the Supreme Court
2 laid the foundation for determining whether a private actor is
3 entitled to qualified immunity. The plaintiff there sued under
4 section 1983 to recover property from a private party who had
5 earlier obtained a writ of replevin against the plaintiff. See
6 Lugar v Edmondson Oil Co, 457 US 922 (1982) (holding that a private
7 party acted under color of law under similar circumstances). After
8 determining that the common law did not recognize an immunity from
9 analogous tort suits, the court "conclude[d] that the rationales
10 mandating qualified immunity for public officials are not
11 applicable to private parties." Wyatt, 504 US at 167. Although
12 Wyatt purported to be limited to its facts, *id* at 168, the broad
13 brush with which the Court painted suggested that private parties
14 could rarely, if ever, don the cloak of qualified immunity. See
15 also Ace Beverage Co v Lockheed Information Mgmt Servs, 144 F3d
16 1218, 1219 n3 (9th Cir 1998) (noting that "[i]n cases decided
17 before [the Supreme Court's decision in Richardson v McKnight, 521
18 US 399 (1997)]," the Ninth Circuit had "adopted a general rule that
19 private parties are not entitled to qualified immunity").

20 Applying Wyatt to a case involving section 1983 claims
21 against privately employed prison guards, the Supreme Court in
22 Richardson v McKnight, 521 US 399 (1997), stated that courts should
23 "look both to history and to the purposes that underlie government
24 employee immunity in order to" determine whether that immunity
25 extends to private parties. *Id* at 404. Although this issue has
26 been addressed by the Ninth Circuit in several cases, the court has
27 yet to extend qualified immunity to a private party under McKnight.
28 See, e g, Ace Beverage, 144 F3d at 1220; Jensen, 222 F3d at 576-80.

The court now determines whether the history of the alleged immunity and purposes of the qualified immunity doctrine support extending qualified immunity to AT&T.

As described in section II(C), *supra*, no firmly rooted common law immunity exists for telecommunications providers assisting the government. And presently applying whatever immunity might have previously existed would undermine the various statutory schemes created by Congress, including the certification defense under 18 USC § 2511(2)(a)(ii)(B).

Turning to the purposes of qualified immunity, they include: "(1) protecting the public from unwarranted timidity on the part of public officials and encouraging the vigorous exercise of official authority; (2) preventing lawsuits from distracting officials from their governmental duties; and (3) ensuring that talented candidates are not deterred by the threat of damages suits from entering public service." Jensen, 222 F3d at 577 (citations, quotations and alterations omitted). See also Harlow, 457 US at 816 (recognizing "the general costs of subjecting officials to the risks of trial — distraction of officials from their governmental duties, inhibition of discretionary action, and deterrence of able people from public service"). AT&T contends that national security surveillance is "a traditional governmental function of the highest importance" requiring access to the "critical telecommunications infrastructure" that companies such as AT&T would be reluctant to furnish if they were exposed to civil liability. AT&T MTD at 17.

//

//

United States District Court
For the Northern District of California

1 AT&T's concerns, while relevant, do not warrant extending
2 qualified immunity here because the purposes of that immunity are
3 already well served by the certification provision of 18 USC §
4 2511(2)(a)(ii). As noted above, although it is unclear whether a
5 valid certification would bar plaintiffs' constitutional claim,
6 section 2511(2)(a)(ii) clearly states that a valid certification
7 precludes the statutory claims asserted here. See *supra* I(G)(1).
8 Hence, but for the government's assertion of the state secrets
9 privilege, the certification provision would seem to facilitate
10 prompt adjudication of damages claims such as those at bar. And
11 because section 2511(2)(a)(ii)'s protection does not appear to
12 depend on a fact-intensive showing of good faith, the provision
13 could be successfully invoked without the burdens of full-blown
14 litigation. Compare Tapley v Collins, 211 F3d 1210, 1215 (11th Cir
15 2000) (discussing the differences between qualified immunity and
16 good faith defense under Title III, 18 USC § 2520(d)).

17 More fundamentally, "[w]hen Congress itself provides for
18 a defense to its own cause of action, it is hardly open to the
19 federal court to graft common law defenses on top of those Congress
20 creates." Berry v Funk, 146 F3d 1003, 1013 (DC Cir 1998) (holding
21 that qualified immunity could not be asserted against a claim under
22 Title III). As plaintiffs suggest, the Ninth Circuit appears to
23 have concluded that the only defense under Title III is that
24 provided for by statute — although, in fairness, the court did not
25 explicitly address the availability of qualified immunity. See
26 Jacobson v Rose, 592 F2d 515, 522-24 (9th Cir 1978) (joined by
27 then-Judge Kennedy). But cf Doe v United States, 941 F2d 780, 797-
28 99 (9th Cir 1991) (affirming grant of qualified immunity from

1 liability under section 504 of the Rehabilitation Act without
2 analyzing whether qualified immunity could be asserted in the first
3 place). Nonetheless, at least two appellate courts have concluded
4 that statutory defenses available under Title III do not preclude a
5 defendant from asserting qualified immunity. Blake v Wright, 179
6 F3d 1003, 1013 (6th Cir 1999) (The court "fail[ed] to see the logic
7 of providing a defense of qualified immunity to protect public
8 officials from personal liability when they violate constitutional
9 rights that are not clearly established and deny them qualified
10 immunity when they violate statutory rights that similarly are not
11 clearly established."); accord Tapley, 211 F3d at 1216. But see
12 Mitchell v Forsyth, 472 US 511, 557 (1985) (Brennan concurring in
13 part and dissenting in part) ("The Court's argument seems to be
14 that the trial court should have decided the legality of the
15 wiretap under Title III before going on to the qualified immunity
16 question, since that question arises only when considering the
17 legality of the wiretap under the Constitution.").

18 With all due respect to the Sixth and Eleventh Circuits,
19 those courts appear to have overlooked the relationship between the
20 doctrine of qualified immunity and the schemes of state and federal
21 official liability that are essentially creatures of the Supreme
22 Court. Qualified immunity is a doctrinal outgrowth of expanded
23 state actor liability under 42 USC § 1983 and Bivens. See Monroe v
24 Pape, 365 US 167 (1961) (breathing new life into section 1983);
25 Scheuer v Rhodes, 416 US 232, 247 (1974) (deploying the phrase
26 "qualified immunity" for the first time in the Supreme Court's
27 jurisprudence); Butz v Economou, 438 US 478 (1978) (extending
28 qualified immunity to federal officers sued under Bivens for

1 federal constitutional violations); Maine v Thiboutot, 448 US 1
2 (1980) (holding that section 1983 could be used to vindicate non-
3 constitutional statutory rights); Harlow, 457 US at 818 (making the
4 unprecedented reference to "clearly established statutory" rights
5 just two years after Thiboutot (emphasis added)). These causes of
6 action "were devised by the Supreme Court without any legislative
7 or constitutional (in the sense of positive law) guidance."

8 Crawford-El v Britton, 93 F3d 813, 832 (DC Cir 1996) (en banc)
9 (Silberman concurring), vacated on other grounds, 523 US 574
10 (1998). "It is understandable then, that the Court also developed
11 the doctrine of qualified immunity to reduce the burden on public
12 officials." Berry, 146 F3d at 1013.

13 In contrast, the statutes in this case set forth
14 comprehensive, free-standing liability schemes, complete with
15 statutory defenses, many of which specifically contemplate
16 liability on the part of telecommunications providers such as AT&T.
17 For example, the Stored Communications Act prohibits providers of
18 "electronic communication service" and "remote computing service"
19 from divulging contents of stored communications. See 18 USC §
20 2702(a)(1), (a)(2). Moreover, the Stored Communications Act
21 specifically contemplates carrier liability for unauthorized
22 disclosure of subscriber records "to any governmental entity." See
23 id § 2702(a)(3). It can hardly be said that Congress did not
24 contemplate that carriers might be liable for cooperating with the
25 government when such cooperation did not conform to the
26 requirements of the act.

27 //

28 //

1 constitutional claim). In United States v United States District
2 Court, 407 US 297 (1972) (Keith), the Supreme Court held that the
3 Fourth Amendment does not permit warrantless wiretaps to track
4 domestic threats to national security, id at 321, reaffirmed the
5 "necessity of obtaining a warrant in the surveillance of crimes
6 unrelated to the national security interest," id at 308, and did
7 not pass judgment "on the scope of the President's surveillance
8 power with respect to the activities of foreign powers, within or
9 without this country," id. Because the alleged dragnet here
10 encompasses the communications of "all or substantially all of the
11 communications transmitted through [AT&T's] key domestic
12 telecommunications facilities," it cannot reasonably be said that
13 the program as alleged is limited to tracking foreign powers.
14 Accordingly, AT&T's alleged actions here violate the constitutional
15 rights clearly established in Keith. Moreover, because "the very
16 action in question has previously been held unlawful," AT&T cannot
17 seriously contend that a reasonable entity in its position could
18 have believed that the alleged domestic dragnet was legal.

19
20 4

21 Accordingly, the court DENIES AT&T's instant motion to
22 dismiss on the basis of qualified immunity. The court does not
23 preclude AT&T from raising the qualified immunity defense later in
24 these proceedings, if further discovery indicates that such a
25 defense is merited.

26 //
27 //
28 //

III

1
2 As this case proceeds to discovery, the court flags a few
3 procedural matters on which it seeks the parties' guidance. First,
4 while the court has a duty to the extent possible to disentangle
5 sensitive information from nonsensitive information, see Ellsberg,
6 709 F2d at 57, the court also must take special care to honor the
7 extraordinary security concerns raised by the government here. To
8 help perform these duties, the court proposes appointing an expert
9 pursuant to FRE 706 to assist the court in determining whether
10 disclosing particular evidence would create a "reasonable danger"
11 of harming national security. See FRE 706(a) ("The court may on
12 its own motion or on the motion of any party enter an order to show
13 cause why expert witnesses should not be appointed, and may request
14 the parties to submit nominations. The court may appoint any
15 expert witnesses agreed upon by the parties, and may appoint expert
16 witnesses of its own selection."). Although other courts do not
17 appear to have used FRE 706 experts in the manner proposed here,
18 this procedural innovation seems appropriate given the complex and
19 weighty issues the court will confront in navigating any future
20 privilege assertions. See Ellsberg, 709 F2d at 64 (encouraging
21 "procedural innovation" in addressing state secrets issues);
22 Halpern, 258 F2d at 44 ("A trial in camera in which the privilege
23 relating to state secrets may not be availed of by the United
24 States is permissible, if, in the judgment of the district court,
25 such a trial can be carried out without substantial risk that
26 secret information will be publicly divulged").

27 //

28 //

1 The court contemplates that the individual would be one
2 who had a security clearance for receipt of the most highly
3 sensitive information and had extensive experience in intelligence
4 matters. This individual could perform a number of functions;
5 among others, these might include advising the court on the risks
6 associated with disclosure of certain information, the manner and
7 extent of appropriate disclosures and the parties' respective
8 contentions. While the court has at least one such individual in
9 mind, it has taken no steps to contact or communicate with the
10 individual to determine availability or other matters. This is an
11 appropriate subject for discussion with the parties.

12 The court also notes that should it become necessary for
13 the court to review additional classified material, it may be
14 preferable for the court to travel to the location of those
15 materials than for them to be hand-carried to San Francisco. Of
16 course, a secure facility is available in San Francisco and was
17 used to house classified documents for a few days while the court
18 conducted its *in camera* review for purposes of the government's
19 instant motion. The same procedures that were previously used
20 could be employed again. But alternative procedures may also be
21 used and may in some instances be more appropriate.

22 Finally, given that the state secrets issues resolved
23 herein represent controlling questions of law as to which there is
24 a substantial ground for difference of opinion and that an
25 immediate appeal may materially advance ultimate termination of the
26 litigation, the court certifies this order for the parties to apply
27 for an immediate appeal pursuant to 28 USC § 1292(b). The court
28 notes that if such an appeal is taken, the present proceedings do

1 not necessarily have to be stayed. 28 USC § 1292(b)
2 ("[A]pplication for an appeal hereunder shall not stay proceedings
3 in the district court unless the district judge or the Court of
4 Appeals or a judge thereof shall so order."). At the very least,
5 it would seem prudent for the court to select the expert pursuant
6 to FRE 706 prior to the Ninth Circuit's review of this matter.

7 Accordingly, the court ORDERS the parties to SHOW CAUSE
8 in writing by July 31, 2006, why it should not appoint an expert
9 pursuant to FRE 706 to assist in the manner stated above. The
10 responses should propose nominees for the expert position and
11 should also state the parties' views regarding the means by which
12 the court should review any future classified submissions.
13 Moreover, the parties should describe what portions of this case,
14 if any, should be stayed if this order is appealed.

15 //
16 //
17 //
18 //
19 //
20 //
21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //

1 IV

2 In sum, the court DENIES the government's motion to
3 dismiss, or in the alternative, for summary judgment on the basis
4 of state secrets and DENIES AT&T's motion to dismiss. As noted in
5 section III, supra, the parties are ORDERED TO SHOW CAUSE in
6 writing by July 31, 2006, why the court should not appoint an
7 expert pursuant to FRE 706 to assist the court. The parties'
8 briefs should also address whether this action should be stayed
9 pending an appeal pursuant to 28 USC § 1292(b).

10 The parties are also instructed to appear on August 8,
11 2006, at 2 PM, for a further case management conference.

12
13 IT IS SO ORDERED.

14 

15
16 VAUGHN R WALKER

17 United States District Chief Judge
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 2

The New York Times
Printer Friendly Format Sponsored By

May 12, 2006

Qwest's Refusal of N.S.A. Query Is Explained
By JOHN O'NEIL and ERIC LICHTBLAU

WASHINGTON, May 12 — The telecommunications company Qwest turned down requests by the National Security Agency for private telephone records because it concluded that doing so would violate federal privacy laws, a lawyer for the telephone company's former chief executive said today.

In a statement released this morning, the lawyer said that the former chief executive, Joseph N. Nacchio, made the decision after asking whether "a warrant or other legal process had been secured in support of that request."

Mr. Nacchio learned that no warrant had been granted and that there was a "disinclination on the part of the authorities to use any legal process," said the lawyer, Herbert J. Stern. As a result, the statement said, Mr. Nacchio concluded that "the requests violated the privacy requirements of the Telecommunications Act."

A Qwest spokesman, Robert Toevs, declined to discuss anything to do with security issues or the statement by Mr. Nacchio's lawyer.

Qwest was the only phone company to turn down requests from the security agency for phone records as part of a program to compile a vast database of numbers and other information on virtually all domestic calls. The program's scope was first described in an article published on Thursday by USA Today that led to an outpouring of demands for information from Congressional Republicans and Democrats. The article said that AT&T, BellSouth and Verizon had agreed to provide the information to the security agency.

On Thursday, those companies said they were following the law in protecting customers' privacy but would not discuss details of the report. Separately today Verizon issued a statement saying that it provided customer information to a government agency "only where authorized by law for appropriately-defined and focused purposes." The company cited unspecified "factual errors in press coverage," about the way it the company handles customer information in general.

The statements came as Gen. Michael V. Hayden, who was the head of the National Security Agency at the time the program began, continued to seek support today for his nomination as C.I.A. director in meetings with senators on Capitol Hill.

Speaking to reporters with Senator Chuck Hagel, Republican of Nebraska, General Hayden declined to comment on the article about the National Security Agency program.

"Everything that the agency has done has been lawful," he said. "It's been briefed to the appropriate members of Congress."

Mr. Hagel, a member of the Intelligence Committee, which will conduct General Hayden's confirmation hearings, said that General Hayden was "the right choice" for the C.I.A.'s top post.

But he also said he supported plans announced Thursday by Senator Arlen Specter, the Republican chairman of the Senate Judiciary Committee, to hold separate hearings into the collection of phone records.

Mr. Hagel called that "appropriate."

"I think this issue needs to be clearly aired," he said. "I think people need to have confidence in their government."

Mr. Hagel said the confirmation hearings would certainly involve "tough questions" for General Hayden. Members of Congress have said they want information both about the collection of phone records and about a program of warrantless wiretaps on calls between people in the United States and people overseas suspected of having ties to terrorism.

The White House continued to express its support of General Hayden today and to sidestep questions about the program to collect telephone records.

Tony Snow, the White House press secretary, told reporters that "we're 100 percent behind Michael Hayden."

Mr. Snow also said that the White House was "confident that he is going to comport himself well and answer all the questions and concerns that members of the United States Senate may have in the process of confirmation."

On Tuesday, President Bush responded to an outcry over the article by assuring the country that "we're not mining or trolling through the personal lives of millions of innocent Americans."

One senior government official, who was granted anonymity to speak publicly about the classified program, confirmed that the N.S.A. had access to records of most telephone calls in the United States. But the official said the call records were used for the limited purpose of tracing regular contacts of "known bad guys."

"To perform such traces," the official said, "you'd have to have all the calls or most of them. But you wouldn't be interested in the vast majority of them."

The New York Times first reported in December that the president had authorized the N.S.A. to conduct eavesdropping without warrants.

The Times also reported in December that the agency had gained the cooperation of American telecommunications companies to get access to records of vast amounts of domestic and international phone calls and e-mail messages.

The agency analyzes communications patterns, the report said, and looks for evidence of terrorist activity at home and abroad.

The USA Today article on Thursday went further, saying that the N.S.A. had created an enormous database of all calls made by customers of the three phone companies in an effort to compile a log of "every call ever made" within this country.

Mr. Nacchio's statement today made a point of saying that the N.S.A. requests occurred "at a time when there was no investigation of Qwest or Mr. Nacchio." Mr. Nacchio, who left Qwest in 2002 amid allegations of fraud at the company, was indicted in December on 42 charges of insider selling.

Prosecutors say Mr. Nacchio did not make investors aware of warnings from his managers that the

company's revenue and profit forecasts were too optimistic. They say Mr. Nacchio kept this information to himself yet also sold 2.5 million shares of Qwest stock over five months in 2001 that netted \$100 million. The case could go to trial later this year. On Thursday, some Republicans, including Representative Peter Hoekstra of Michigan, chairman of the House Intelligence Committee, defended the N.S.A.'s activities and denounced the disclosure. Mr. Hoekstra said the report "threatens to undermine our nation's safety."

"Rather than allow our intelligence professionals to maintain a laser focus on the terrorists, we are once again mired in a debate about what our intelligence community may or may not be doing," he said.

But many Democrats and civil liberties advocates said they were disturbed by the report, invoking images of Big Brother and announcing legislation aimed at reining in the N.S.A.'s domestic operations. Fifty-two members of Congress asked the president to name a special counsel to investigate the N.S.A.'s domestic surveillance programs.

Senator Arlen Specter, the Pennsylvania Republican who heads the Judiciary Committee, said the reported data-mining activities raised serious constitutional questions. He said he planned to seek the testimony of telephone company executives.

The House majority leader, John A. Boehner of Ohio, said he wanted more information on the program because "I am not sure why it would be necessary to keep and have that kind of information."

Mr. Bush did not directly confirm or deny the existence of the N.S.A. operation but said that "as a general matter, every time sensitive intelligence is leaked it hurts our ability to defeat this enemy."

Seeking to distinguish call-tracing operations from eavesdropping, the president said that "the government does not listen to domestic phone calls without court approval."

The phone records include numbers called; time, date and direction of calls; and other details, but not the words spoken, telecommunications experts said. Customers' names and addresses are not included in the companies' call records, though they could be cross-referenced to obtain personal data.

The law on data-mining activities is murky, and legal analysts were divided Thursday on the question of whether the N.S.A.'s tracing and analysis of huge streams of American communications data would require the agency to use subpoenas or court warrants.

Kate Martin, director of the Center for National Security Studies, said, "If they don't get a court order, it's a crime." Ms. Martin said that while the F.B.I. might be able to get access to phone collection databases by using an administrative subpoena, her reading of federal law was that the N.S.A. would be banned from doing so without court approval.

But another expert on the law of electronic surveillance, Kenneth C. Bass III, said that if access to the call database was granted in response to a national security letter issued by the government, "it would probably not be illegal, but it would be very troubling."

"The concept of the N.S.A. having near-real-time access to information about every call made in the country is chilling," said Mr. Bass, former counsel for intelligence policy at the Justice Department. He said the phone records program resembled Total Information Awareness, a Pentagon data-mining program shut down by Congress in 2003 after a public outcry.

The N.S.A. refused to discuss the report, but said in a statement that it "takes its legal responsibilities

seriously and operates within the law."

AT&T, Verizon and BellSouth all issued statements saying they had followed the law in protecting customers' privacy but would not discuss details of the report.

"AT&T has a long history of vigorously protecting customer privacy," said Selim Bingol, a company spokesman. "We also have an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare."

Mr. Specter said in an interview that he would press for information on the operations of the N.S.A. program to determine its legality.

"I don't think we can really make a judgment on whether warrants would be necessary until we know a lot more about the program," he said.

One central question is whether the N.S.A. uses its analysis of phone call patterns to select people in the United States whose phone calls and e-mail messages are monitored without warrants. The Times has reported that the agency is believed to have eavesdropped on the international communications of about 400 to 500 people at a time within the United States and of thousands of people since the Sept. 11 attacks.

Democrats said they would use the new disclosures to push for more answers from General Hayden at his confirmation hearing, set for May 18.

Senator Dianne Feinstein, Democrat of California, predicted "a major Constitutional confrontation on Fourth Amendment guarantees of unreasonable search and seizure" and said the new disclosures presented "a growing impediment to the confirmation of General Hayden."

Scott Shane contributed reporting from Washington for this article.

Home

- * World
- * U.S.
- * N.Y. / Region
- * Business
- * Technology
- * Science
- * Health
- * Sports
- * Opinion
- * Arts
- * Style
- * Travel
- * Jobs
- * Real Estate
- * Automobiles
- * Back to Top

Copyright 2006 The New York Times Company

- * Privacy Policy

- * [Search](#)
- * [Corrections](#)
- * [XML](#)
- * [Help](#)
- * [Contact Us](#)
- * [Work for Us](#)
- * [Site Map](#)

EXHIBIT 3



Verizon: We Didn't Give Customers' Call Records to NSA Either

Tuesday, May 16, 2006

Associated Press

NEW YORK — Verizon Communications Inc. denied Tuesday that it had received a request for customer phone records from the National Security Agency, bringing into question key points of a USA Today story.

"Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records," the New York-based phone company said in an e-mailed statement.

The statement came a day after BellSouth Corp. also said the NSA had never requested customer call data, nor had the company provided any.

• [Click here to read the USA Today article.](#)

A story in USA Today last Thursday said Verizon, AT&T Inc. and BellSouth had complied with an NSA request for tens of millions of customer phone records after the 2001 terror attacks. The report sparked a national debate on federal surveillance tactics.

The newspaper story cited anonymous sources "with direct knowledge of the arrangement."

"Sources told us that BellSouth and Verizon records are included in the database," USA Today spokesman Steve Anderson said Tuesday.

"We're confident in our coverage of the phone database story," Anderson added, "but we won't summarily dismiss BellSouth's and Verizon's denials without taking a closer look."

USA Today said in a follow-up story Tuesday that BellSouth did not challenge the initial report when given details about it before publication. But BellSouth spokesman Jeff Battcher said he never agreed to the reporter's allegations when presented with them.

Verizon also said USA Today erred in not drawing a distinction between long-distance and local telephone calls.

"Phone companies do not even make records of local calls in most cases because the vast majority of customers are not billed per call for local calls," Verizon's statement said.

Three smaller phone companies, with mainly local business, contacted by The Associated Press on Tuesday also denied being approached by the NSA. Representatives at Alltel Corp., Citizens Communications Co. and CenturyTel Inc. all said they had no knowledge of NSA requests to their companies.

Verizon's statement Tuesday apparently did not apply to MCI, which Verizon acquired in January. In an earlier statement, Verizon said it is in the process of ensuring that its policies are put in place in the former MCI business.

MCI had a long-distance consumer business, but its main source of revenue was corporate clients.

It's as easy as
1, 2, 3!

**ORDER
NOW**

An attorney for the former chief executive of Qwest Communications International Inc., another regional phone company, said Friday that the company had been approached by the government, but denied the request for phone records because it appeared to violate privacy law.

The denials by Verizon and BellSouth leaves AT&T as the sole company named in the USA Today article that hasn't denied involvement. On Thursday, San Antonio-based AT&T said it had "an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare," but said would only assist as allowed within the law.

AT&T spokesman Michael Coe said Tuesday the company had no further comment.

BellSouth, Verizon and AT&T are facing a number of lawsuits by customers who allege violations of their privacy. On Monday, a Democratic member of the Federal Communications Commission said the FCC whether the companies are violating federal communications law.

SEARCH

GO

[Click here for FOX News RSS Feeds](#)

Advertise on FOX News Channel, FOXNews.com and FOX News Radio

Jobs at FOX News Channel.

Internships at FOX News Channel (now accepting Fall interns).

Terms of use. Privacy Statement. For FOXNews.com comments write to foxnews@foxnews.com; For FOX News Channel comments write to comments@foxnews.com

© Associated Press. All rights reserved.

This material may not be published, broadcast, rewritten, or redistributed.

Copyright 2006 FOX News Network, LLC. All rights reserved.

All market data delayed 20 minutes.

THE GALLUP POLL®

SOURCE: Gallup Poll News Service

CONTACT INFORMATION: Media Relations 1-202-715-3030

Subscriber Relations 1-888-274-5447

Gallup World Headquarters

901 F Street, NW

Washington, D.C. 20004

Civil Liberties

Gallup's Pulse of Democracy

The Patriot Act and Civil Liberties

Guidance for Lawmakers In general, a majority of Americans have been comfortable with the current level of government intrusion on civil liberties as part of the war on terrorism. The strong majority of Americans believe the Patriot Act needs only minor changes, at best. Slightly less than one-third would make major changes or eliminate the law completely.

Recent revelations about the National Security Agency's collection of phone records of millions of Americans and government wiretapping have met with mixed reactions. Research suggests that a slight majority of Americans disapprove of the NSA program, while most polling showed that a slight majority of Americans accepted the wiretapping as legitimate.

In the most general sense, Americans appear torn between the desire to fight terrorism and protect civil liberties, and each new revelation of what the government has done since 9/11 is evaluated in that context. This balance between civil liberties and fighting terrorism becomes the major focus of policy decisions in this area.

Fine Print Numerous polling organizations have asked Americans for their views on civil liberties, the Patriot Act, wiretapping, and the government's collection of massive telephone records. The results produce mixed results depending on what is emphasized within the question. Polls on the one hand find some reluctance to give up civil liberties and concern about how far the government will go in this regard. On the other hand, polls that stress the positive aspects of the Patriot Act or positive reasons for restricting civil liberties find greater public support than those that do not.

It is important to be cautious in placing too much emphasis on the results of any one poll question measuring public opinion in this area.

Context The issue of civil liberties came to the forefront of the political spectrum

after the 9/11 terrorist attacks. In the years since 9/11, however, Americans have become less willing to sacrifice their civil liberties -- even to combat terrorism. Public opinion has become more partisan as it has become clearer that the Republican Bush administration has undertaken significant programs in its efforts to fight terrorism.

Urgency: Overall A January 2006 poll showed that dealing with the Patriot Act and **Importance as Political Issue** government surveillance of U.S. citizens ranked at or near the bottom of a list of potential priorities for Congress. Slightly more than one in four Americans say the Patriot Act will be extremely important to their votes for Congress this fall. Fewer than 3 in 10 Americans say government surveillance of U.S. citizens is extremely important to their votes. Few Americans mention privacy or civil liberties concerns as the most important problem facing the country.

Impact on Bush, Politics Americans continue to give the president's overall handling of civil liberties the benefit of the doubt. More than half of Americans say the Bush administration has been about right or has not gone far enough in restricting people's civil liberties in order to combat terrorism. However, there has been a steady increase since 2002 in the percentage saying the administration has gone too far in this regard, now at a high of 41%.

Americans are more negative than positive in their initial assessment of the government program to obtain telephone records from the three largest U.S. telephone companies as an effort to combat terrorism. It is unclear what part this issue will play for the president or in the 2006 midterm elections.

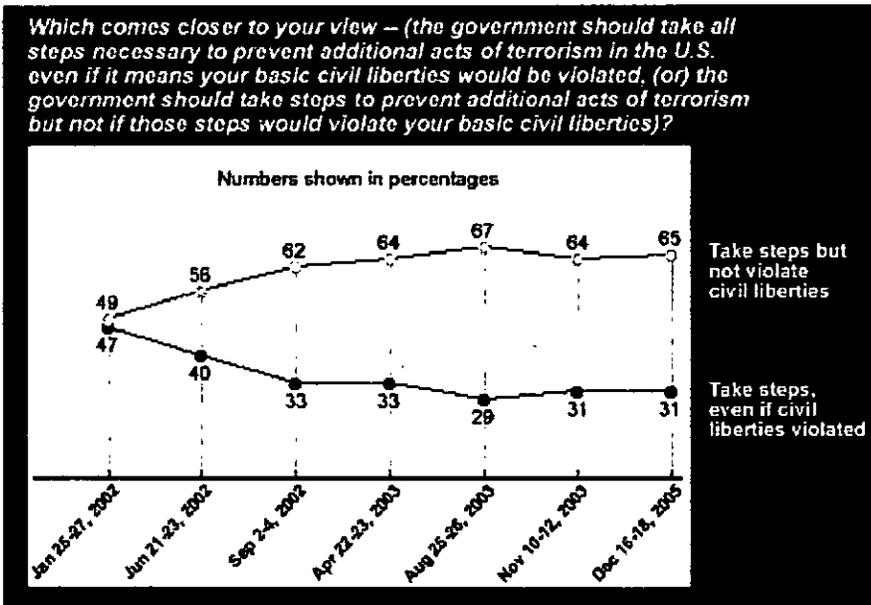
Key Subgroup Differences Views about the Patriot Act and civil liberties are highly partisan.

The vast majority of Democrats say the Bush administration has gone too far in restricting civil liberties in order to combat terrorism, while Republicans say the administration has been about right or has not gone far enough in this regard.

Republicans are also more willing than Democrats to say the government should take whatever steps are necessary to prevent future acts of terrorism even if basic civil liberties are violated.

Republicans are more likely than Democrats to favor recently revealed government programs involved with wiretapping and collection of telephone numbers.

The Bottom Line Americans do not believe the government should violate citizens' basic civil liberties in order to combat terrorism. At the same time, most Americans do not think the Bush administration has gone too far restricting civil liberties to fight the war on terror. The balance between liberties and fighting terrorism is the important determinant of attitudes in this issue area. Most recently, polling shows that more than half of Americans object to the government program that obtains records from three of the largest U.S. telephone companies to create a database of billions of telephone numbers dialed by Americans. Dealing with the Patriot Act per se has a low priority for Americans, although terrorism remains a very high priority.



As you may know, the Bush administration has been wiretapping telephone conversations between U.S. citizens living in the United States and suspected terrorists living in other countries without getting a court order allowing it to do so. Do you think the Bush administration was right or wrong in wiretapping these conversations without obtaining a court order?

	Right	Wrong	No opinion
2006 Sep 15-17	55%	42	3
2006 Feb 9-12 ^	47%	50	3
2006 Jan 20-22 ^	46%	51	3
2006 Jan 6-8	50%	46	4

^ Asked of a half sample.

As you may know, in the U.S. legal system the government is required to show defendants the evidence it has against them. In some terrorism trials, the government believes that showing defendants certain evidence may put American lives in danger. In your view, which would be worse -- [ROTATED: convicting defendants of terrorism based on evidence they are never shown, (or) having some terrorism suspects go free because the government chooses to withhold evidence rather than show it to the defendant]?

	Convicting defendants on evidence they are never shown	Letting some terrorists go free	No opinion
2006 Sep 15-17	48%	41	11

When interrogating prisoners, members of the U.S. military are required to abide by the Geneva Convention standards which prohibit the humiliating and degrading treatment of prisoners. When the CIA or Central Intelligence Agency questions suspects whom they believe to have information about possible terror plots against the United States, do you think -- [ROTATED: they should have to abide by the same Geneva Convention standards that apply to the U.S. military (or) they should be able to use more forceful interrogation techniques than the Geneva Convention standards that apply to the U.S. military]?

	Abide by Geneva Convention standards	Able to use more forceful techniques	Other/depends (vol.)	No opinion
2006 Sep 15-17	57%	38	2	3

Do you think the Bush administration – [ROTATED: has gone too far, has been about right, or has not gone far enough] – in restricting people's civil liberties in order to fight terrorism?]

	Too far %	About right %	Not far enough %	No opinion %
2006 May 12-13	41	34	19	6
2006 Jan 6-8	38	40	19	3
2003 Nov 10-12 ^	28	48	21	3
2003 Aug 25-26 ^	21	55	19	5
2002 Sep 2-4 ^	15	55	26	4
2002 Jun 21-23 ^	11	60	25	4

^ Asked of a half sample.

As you may know, as part of its efforts to investigate terrorism, a federal government agency obtained records from three of the largest U.S. telephone companies in order to create a database of billions of telephone numbers dialed by Americans. How closely have you been following the news about this – very closely, somewhat closely, not too closely, or not at all?

	Very closely	Some-what closely	Not too closely	Not at all	No opinion
2006 May 12-13	28%	39	20	12	*

Based on what you have heard or read about this program to collect phone records, would you say you approve or disapprove of this government program?

	Approve	Disapprove	No opinion
2006 May 12-13	43%	51	6

Is that mainly because – [ROTATED: you do not think the program seriously violates Americans' civil liberties, (or is it mainly because) you think investigating terrorism is the more important goal, even if it violates some Americans' civil liberties]

[ASKED OF ADULTS WHO APPROVE OF GOVERNMENT PROGRAM]

	Does not seriously violate civil liberties	Terrorism more important, even if violates civil liberties	No opinion
2006 May 12-13	27%	69	4

A. Based on this program, the government would listen in on telephone conversations within the U.S. without first obtaining a warrant

	Very concerned	Some-what concerned	Not too concerned	Not concerned at all	No opinion
2006 May 12-13	41%	22	17	19	1

B. The government is gathering other information on the general public, such as their bank records or Internet usage

	Very concerned	Some-what concerned	Not too concerned	Not concerned at all	No opinion
2006 May 12-13	45%	22	15	17	1

As you may know, shortly after the terrorist attacks on September 11, 2001, a law called the Patriot Act was passed which makes it easier for the federal government to get information on suspected terrorists through court-ordered wiretaps and searches. How familiar are you with the Patriot Act -- very familiar, somewhat familiar, not too familiar, or not at all familiar?

	Very familiar	Somewhat familiar	Not too familiar	Not at all familiar	No opinion
2006 Jan 6-8	17%	59	18	6	*
2004 Feb 16-17	13%	46	27	14	*
2003 Nov 10-12 ^	12%	41	25	22	*
2003 Aug 25-26 ^	10%	40	25	25	--

^ Asked of a half sample.

Based on what you have heard or read about the Patriot Act, do you think -- [ROTATED: all of its provisions should be kept, that it needs minor changes, that it needs major changes, (or that) it needs to be eliminated completely]?

	Keep all provisions	Minor changes	Major changes	Eliminated completely	No opinion
2006 Jan 6-8	13%	50	24	7	7

As you may know, shortly after the terrorist attacks on September 11, 2001, a law called the Patriot Act was passed. That law deals with the ways the federal government can obtain private information on people living in the U.S. who are suspected of having ties with terrorists. Based on what you have read or heard, do you think the Patriot Act -- [ROTATED: goes too far, is about right, or does not go far enough] -- in restricting people's civil liberties in order to investigate suspected terrorism?

	Goes too far	About right	Not far enough	No opinion
2005 Dec 16-18 ^	34%	44	18	4
2005 Jun 24-26	30%	41	21	8

^ Asked of a half sample.

Which comes closer to your view -- [ROTATED: the government should take all steps necessary to prevent additional acts of terrorism in the U.S. even if it means your basic civil liberties would be violated, (or) the government should take steps to prevent additional acts of terrorism but not if those steps would violate your basic civil liberties]?

	Take steps, even if civil liberties violated	Take steps but not violate civil liberties	No opinion
	%	%	%
2005 Dec 16-18 ^	31	65	4
2003 Nov 10-12 ^	31	64	5
2003 Aug 25-26 ^	29	67	4
2003 Apr 22-23	33	64	3
2002 Sep 2-4 ^	33	62	5
2002 Jun 21-23	40	56	4
2002 Jan 25-27	47	49	4

^ Asked of a half sample.

As you may know, shortly after the terrorist attacks on September 11, 2001, a law called the Patriot Act was passed. That law deals with the ways the federal government can obtain private information on people living in the U.S. who are suspected of having ties with terrorists. How familiar are you with the Patriot Act -- very familiar, somewhat familiar, not too familiar, or not at all familiar?

	Very familiar	Somewhat familiar	Not too familiar	Not at all familiar	No opinion
2005 Jun 24-26	12%	52	25	11	--

Next, I will read a list of things government officials can do when conducting a terrorism investigation. For each, please tell me if this is something government officials can do specifically because of the Patriot Act, or if it is something they could have done prior to the Patriot Act being passed. How about -- [RANDOM ORDER]?

[BASED ON -505--NATIONAL ADULTS IN FORM A]

A. Hold terrorism suspects indefinitely without charging them with a crime or allowing them access to a lawyer

	Can do because of the Patriot Act	Could do before Patriot Act passed	No opinion
2004 Feb 16-17	60%	26	14

B. Require non-U.S. citizens who are suspected of terrorism offenses to face a trial before a military tribunal

	Can do because of the Patriot Act	Could do before Patriot Act passed	No opinion
--	--------------------------------------	---------------------------------------	---------------

2004 Feb 16-17	51%	34	15
----------------	-----	----	----

C. Enter houses of worship or attend political rallies

	Can do because of the Patriot Act	Could do before Patriot Act passed	No opinion
2004 Feb 16-17	28%	54	18

One provision in the Patriot Act allows federal agents to secretly search a U.S. citizen's home without informing the person of that search for an unspecified period of time. Do you approve or disapprove of this provision?

[BASED ON -501—NATIONAL ADULTS IN FORM B]

	Approve	Disapprove	No opinion
2004 Feb 16-17	26%	71	3

Another provision in the Patriot Act requires businesses, including hospitals, bookstores, and libraries, to turn over records in terrorism investigations and prevents the businesses from revealing to their patients or clients that these records have been turned over to the government. Do you approve or disapprove of this provision?

[BASED ON -501—NATIONAL ADULTS IN FORM B]

	Approve	Disapprove	No opinion
2004 Feb 16-17	45%	51	4

One provision of the Patriot Act allows federal agents in terrorism or money-laundering investigations to submit lists of people to financial institutions. The institutions are required to reveal whether the people on the lists have accounts with them. The federal agents can submit the names without a judge's prior approval. Do you approve or disapprove of this provision?

[BASED ON -501—NATIONAL ADULTS IN FORM B]

	Approve	Disapprove	No opinion
2004 Feb 16-17	51%	45	4

[^ Back to Top](#)



Copyright © 2007 The Gallup Organization, Princeton, NJ. All rights reserved. Gallup®, A™, Business Impact A Clifton StrengthsFinder®, the 34 Clifton StrengthsFinder theme names, Customer Engagement Index™, Drop Ci Economy™, Employee Engagement Index™, Employee Outlook Index™, Follow This Path™, Gallup Brain™, Ga Gallup Management Journal®, GMJ®, Gallup Press™, Gallup Publishing™, Gallup Tuesday Briefing®, Gallup Uni HumanSigma®, I™, L™, PrincipallInsight™, Q™, SE™, SF™, SRI®, Strengths Spotlight™, Strengths-Based S StrengthsCoach™, StrengthsFinder®, StrengthsQuest™, TeacherInsight™, The Gallup Path®, and The Gallup Pr The Gallup Organization. All other trademarks are the property of their respective owners. These materials are noncommercial, personal use only. Reproduction prohibited without the express permission of The Gallup Orga

EXHIBIT 5

RasmussenReports.com - <http://www.rasmussenreports.com/2005/NSA.htm>

December 28, 2005--Sixty-four percent (64%) of Americans believe the National Security Agency (NSA) should be allowed to intercept telephone conversations between terrorism suspects in other countries and people living in the United States. A Rasmussen Reports survey found that just 23% disagree.

Sixty-eight percent (68%) of Americans say they are following the NSA story somewhat or very closely.

Just 26% believe President Bush is the first to authorize a program like the one currently in the news. Forty-eight percent (48%) say he is not while 26% are not sure.

Eighty-one percent (81%) of Republicans believe the NSA should be allowed to listen in on conversations between terror suspects and people living in the United States. That view is shared by 51% of Democrats and 57% of those not affiliated with either major political party.

Rasmussen Reports is an electronic publishing firm specializing in the collection, publication, and distribution of public opinion polling information.

The Rasmussen Reports ElectionEdge™ Premium Service for Election 2006 offers the most comprehensive public opinion coverage ever provided for a mid-term election. We will poll every Senate and Governor's race at least once a month.

Rasmussen Reports was the nation's most accurate polling firm during the Presidential election and the only one to project both Bush and Kerry's vote total within half a percentage point of the actual outcome.

During Election 2004, RasmussenReports.com was also the top-ranked public opinion research site on the web. We had twice as many visitors as our nearest competitor and nearly as many as all competitors combined.

Scott Rasmussen, president of Rasmussen Reports, has been an independent pollster for more than a decade.

The telephone survey of 1,000 Adults was conducted by Rasmussen Reports December 26-27, 2005. The margin of sampling error for the survey is +/- 4.5 percentage points at the midpoint with a 95% level of confidence (see Methodology).

EXHIBIT 6

Media Reports on AT&T's involvement in the Programs

Print and Electronic

1. Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 11, 2006
2. John O'Neil and Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained*, New York Times, May 12, 2006
3. Ken Belson and Matt Richtel, *Verizon Denies Turning Over Local Phone Data*, The New York Times, May 17, 2006
4. Matt Richtel and Ken Belson, *U.S. Focused on Obtaining Long-Distance Phone Data, Company Officials Indicate*, New York Times, May 18, 2006
5. Evan Hansen, *Why We Published the AT&T Docs*, Wired News, May 22, 2006
6. Michael Higgins, *ACLU Sues AT&T Over Phone Records*, Chicago Tribune, May 20, 2006
7. Anthony D. Romero, *A Little Straight Talk, Please, on the NSA Scandal*, Salt Lake Tribune, May 20, 2006
8. Marcia Coyle, *The Fight Over Phone Records*, National Law Journal, May 22, 2006
9. Studs Terkel, *Other Sue AT&T Over Release of Records*, Associated Press, May 23, 2006
10. Larry Neumeister, *ACLU Seeks to Rally Population Against Govt's Phone Snooping*, Associated Press, May 23, 2006
11. Peter Grier, *For Telecoms, a Storm of Lawsuits Awaits*, Christian Science Monitor, May 24, 2006
12. Larry Neumeister, *ACLU Files Complaints Over Government Phone Snooping*, Associated Press, May 25, 2006
13. Editorial, *Make No Law*, Washington Post, May 25, 2006
14. Ryan Kim, *INSECURITY: Bugged by Phone Companies*, San Francisco Chronicle, May 25, 2006
15. Kathleen Burge, *Mayors Demand Phone Inquiry*, Boston Globe, May 25, 2006
16. Michael D. Sorkin, *AT&T Broke Privacy Laws, Suit Here Says*, St. Louis Post-Dispatch (Missouri), May 25, 2006

17. Darren M. Allen, *ACLU Files Complaint Over Phone Records*, Rutland Herold (Vermont), May 25, 2006
18. Paul Shukovsky, *ACLU in State Wants Phone Firms Checked*, Seattle Post Intelligencer, May 25, 2006
19. Ian Martinez, *ACLU Attacks Wiretapping at State Level*, Communications Daily, May 25, 2006
20. Mary Schmich and Eric Zorn, *Is it a Big Deal if the Feds Have Your Number?*, Chicago Tribune, May 25, 2006
21. John Diamond, *Specter: Cheney put pressure on panel*, USA Today, June 7, 2006
22. John Diamond, *Senators won't grill phone companies*, USA Today, June 7, 2006
23. Ryan Singel, *AT&T: Wired News Is a 'Scofflaw'*, Wired News, June 13, 2006
24. Scott Lindlaw, *SF Reviews Contracts with AT&T Over Domestic Spying*, Associated Press, July 11, 2006
25. Ryan Singel, *Judge: NSA Case Can Proceed*, Wired News, July 20, 2006
26. Roger Cheng, *Judge Denies AT&T, U.S. Motion to Dismiss Domestic Spying Case*, Wall Street Journal, July 21, 2006
27. Declan McCullagh, *AT&T says cooperation with NSA could be legal*, CNET News.com, August 22, 2006
28. Katie Zezima, *Maine: Lawsuit Over Phone Records*, New York Times, September 22, 2006
29. Ryan Singel, *NSA Case Becomes Lawyer Junket*, Wired News, November 17, 2006
30. Declan McCullagh, *Judge won't halt AT&T wiretapping lawsuit*, CNET News.com, November 18, 2006
31. Onnesha Roychoudhuri, *DoJ Quashes Wiretapping Inquiries*, In These Times (Illinois) November 20, 2006
32. Lisle Brunner, *DOJ asks appeals court to block domestic surveillance lawsuit*, Jurist, December 5, 2006

Radio

1. Larry Abramson, *Phone Companies Deny Cooperating with NSA*, Weekend Edition, **National Public Radio**, May 20, 2006
2. Story, Morning Edition, **National Public Radio**, May 24, 2006
3. O. Kay Henderson, *ICLU Jumps Into Phone Records Debate*, **Radio Iowa**, May 24, 2006
4. Larry Abramson, Morning Edition, **National Public Radio**, May 25, 2006
5. Armstrong Williams and Sam Greenfield, WWRL Morning Show, **WWRL 1600**, May 25, 2006

Television

1. **MSNBC**, Dan Abrams Report, May 24, 2006
2. **CBS News**, The Early Show, May 24, 2006
3. **CNN**, News Report, May 25, 2006
4. **CNBC**, Morning Call, May 25, 2006

RasmussenReports.com - <http://www.rasmussenreports.com/2005/NSA.htm>

December 28, 2005--Sixty-four percent (64%) of Americans believe the National Security Agency (NSA) should be allowed to intercept telephone conversations between terrorism suspects in other countries and people living in the United States. A Rasmussen Reports survey found that just 23% disagree.

Sixty-eight percent (68%) of Americans say they are following the NSA story somewhat or very closely.

Just 26% believe President Bush is the first to authorize a program like the one currently in the news. Forty-eight percent (48%) say he is not while 26% are not sure.

Eighty-one percent (81%) of Republicans believe the NSA should be allowed to listen in on conversations between terror suspects and people living in the United States. That view is shared by 51% of Democrats and 57% of those not affiliated with either major political party.

Rasmussen Reports is an electronic publishing firm specializing in the collection, publication, and distribution of public opinion polling information.

The Rasmussen Reports ElectionEdge™ Premium Service for Election 2006 offers the most comprehensive public opinion coverage ever provided for a mid-term election. We will poll every Senate and Governor's race at least once a month.

Rasmussen Reports was the nation's most accurate polling firm during the Presidential election and the only one to project both Bush and Kerry's vote total within half a percentage point of the actual outcome.

During Election 2004, RasmussenReports.com was also the top-ranked public opinion research site on the web. We had twice as many visitors as our nearest competitor and nearly as many as all competitors combined.

Scott Rasmussen, president of Rasmussen Reports, has been an independent pollster for more than a decade.

The telephone survey of 1,000 Adults was conducted by Rasmussen Reports December 26-27, 2005. The margin of sampling error for the survey is +/- 4.5 percentage points at the midpoint with a 95% level of confidence (see Methodology).



NEWS

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: <http://www.fcc.gov>
TTY: 1-888-835-5322

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action.
See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).

FOR IMMEDIATE RELEASE
May 15, 2006

NEWS MEDIA CONTACT:
Jessica Rosenworcel: (202) 418-2000

COMMISSIONER MICHAEL J. COPPS CALLS FOR THE FCC TO OPEN AN INQUIRY INTO THE LAWFULNESS OF THE DISCLOSURE OF AMERICA'S PHONE RECORDS

Washington, D.C.—Reacting to recent news reports that the nation's largest telecommunications carriers provided the government with customers' calling records, Commissioner Michael J. Copps stated:

“Recent news reports suggest that some – but interestingly not all – of the nation’s largest telephone companies have provided the government with their customers’ calling records. There is no doubt that protecting the security of the American people is our government’s number one responsibility. But in a Digital Age where collecting, distributing, and manipulating consumers’ personal information is as easy as a click of a button, the privacy of our citizens must still matter. To get to the bottom of this situation, the FCC should initiate an inquiry into whether the phone companies’ involvement violated Section 222 or any other provisions of the Communications Act. We need to be certain that the companies over which the FCC has public interest oversight have not gone – or been asked to go – to a place where they should not be.”

--FCC--

EXHIBIT 8

EDWARD J. MARKEY

7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE

RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States

House of Representatives

Washington, DC 20515-2107

May 15, 2006

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-2107
(202) 225-2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900
www.house.gov/markey

The Honorable Kevin Martin
Chairman, Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dear Mr. Chairman:

I am writing with respect to recent media reports about a massive program at the National Security Agency (NSA) designed to collect the telephone records of millions of Americans. According to these media reports, some of our nation's largest telecommunications carriers, namely AT&T, Verizon, and BellSouth, are working with that intelligence agency and disclosing to the NSA customer telephone calling information.

As you know, Section 222 of the Communications Act of 1934 (47 U.S.C. 222) contains prohibitions on the disclosure of such information by telecommunications carriers. Specifically, Section 222(a) states the following:

"In General – Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications services provided by a telecommunications carrier." (Emphasis added.)

The revelation that several telecommunications carriers are complicit in the NSA's once-secret program, raises the question as to whether these carriers are in violation of Section 222 of the Communications Act and the Commission's regulations implementing that section. As you know, one of the principal purposes of Section 222 is to safeguard the privacy of telecommunications consumers. I am aware of no exception in that statute or in the Commission's regulations for "intelligence gathering purposes," or any other similar purpose, that would permit the wholesale disclosure of consumer records to any entity.

Also, at least one telecommunications carrier, Qwest, objected to participating in the NSA program. According to reports, it refused because it allegedly believed the program was illegal and violated the Communications Act.

The Honorable Kevin Martin

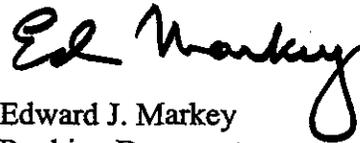
May 15, 2006

Page Two

I would like to know what the Commission intends to do with respect to probing these apparent breaches of the customer privacy provisions of the Communications Act. Please provide me with a response which outlines the Commission's plan, in detail, for investigating and resolving these alleged violations of consumer privacy. In the alternative, please provide detailed legal reasoning as to why the Commission believes the NSA program, as described, is not violative of the law or the Commission's regulations and why the Commission is therefore not taking any enforcement action. I respectfully request a response to this inquiry by close of business on Monday, May 22, 2006.

Thank you in advance for your attention to this matter.

Sincerely,

A handwritten signature in black ink that reads "Ed Markey". The signature is written in a cursive style with a large, looping "E" and "M".

Edward J. Markey

Ranking Democrat

House Subcommittee on

Telecommunications and the Internet

EXHIBIT 9

STATE OF VERMONT
PUBLIC SERVICE BOARD

Docket No. 7193

Petition of Vermont Department of Public)
Service for an investigation into alleged)
unlawful customer records disclosure by AT&T)
Communications of New England, Inc.)

Order entered: 9/18/2006

ORDER ON MOTION TO DISMISS

SUMMARY

This Order denies AT&T's motion to dismiss. We have jurisdiction under state law to proceed in this matter, and it has not been shown that federal law preempts that jurisdiction. Notwithstanding the many bases upon which AT&T asserts that the claims here are preempted by federal law, we conclude that the Department of Public Service may still be able to adduce facts that sustain at least some of its claims. We recognize that discovery in this case may be limited, but we allow the Department to seek to prove its case by whatever unprivileged evidence it can glean from discovery of AT&T and from whatever other reliable sources that may develop.

Based on the record before us, we conclude that the state secrets privilege does not apply here, largely because it has not been properly claimed, but also because it would not apply to all claims. We also conclude that dismissal is not required by the National Security Agency statute, the Foreign Intelligence Surveillance Act, the statutes and rules regarding classified information, or the Intelligence Reform and Terrorism Prevention Act of 2004.

TABLE OF CONTENTS

I. Background	3
The Petition	3
The Motions To Dismiss	4
Participation by the United States Government	8
Responses by the Department	9
AT&T's Reply	11
II. Discussion	12
Standard for Motions to Dismiss	12
State Law - Public Service Board Jurisdiction	13
Federal Law	14
State Secrets	14
Justiciability of Claims	14
Evidentiary Privilege	16
Field Preemption	19
Statutory Arguments	20
The NSA Statute	20
Foreign Intelligence Surveillance Act	22
Classified Information	23
Intelligence Reform and Terrorism Prevention Act of 2004	26
III. Conclusion	26

I. BACKGROUND

The Petition

This docket was commenced to examine whether AT&T Communications of New England, Inc. ("AT&T") violated Vermont utility standards by disclosing customer record information to the National Security Agency ("NSA") or other federal or state agencies¹ ("NSA Customer Records Program"). It was initiated by petition of the Vermont Department of Public Service ("Department") filed on June 21, 2006. The petition reported that the Department had sought information from AT&T, but that AT&T's response did "not even attempt to answer" the questions posed by the Department. The petition alleges that this has obstructed the Department in its statutory duties and that any disclosures to the NSA, if they have occurred, would have violated state and federal laws. The petition concludes by requesting that penalties be imposed on AT&T for its failure to adequately respond and any further relief that the Board deems proper.

Attached to the petition was a copy of the Department's information request, dated May 17, 2006, and a brief response letter from AT&T, dated May 25, 2006. In AT&T's letter, it asserts that it "does not give customer information to law enforcement authorities or government agencies without legal authorization" and that any release of information to law enforcement officials, occurs "strictly within the law." The letter also states that "matters of national security . . . must be addressed on a national basis."

There are no allegations that AT&T was coerced into participating in the NSA Customer Records Program. It has been reported that one major Bell company, Qwest, elected not to participate.² The Department's discovery request and petition have raised the following questions of fact:

1. Whether AT&T participated in the NSA Customer Records Program.

1. The Department also sought information from AT&T regarding similar disclosures to any other federal or state agency. In the text below, "NSA Customer Records Program" should be read as including disclosures to and activity by any state or federal agency, including but not limited to the NSA.

2. According to counsel for Qwest's former Chief Executive Officer Joseph Nacchio, the government approached Mr. Nacchio several times between the fall of 2001 and the summer of 2002 to request its customer telephone records, but because the government failed to cite any legal authorization in support of its demands, Mr. Nacchio refused the requests. See John O'Neil, *Qwest's Refusal of N.S.A. Query Is Explained*, N.Y. Times, May 12, 2006. Quoted in *Terkel v. AT&T Corp.*, ___ F.Supp. ___, 2006 WL 2088202, slip op. at 23 (N.D.Ill. July 25, 2006) (hereafter "*Terkel*").

2. If AT&T did participate:
 - a. What kinds of information were provided, for how many customers, in what form and when?
 - b. Did AT&T modify its equipment in Vermont to participate?
 - c. Did AT&T act voluntarily? Did it act in response to an exercise of governmental authority?
 - d. Did AT&T receive compensation? If so, how much? How much is attributable to Vermont?
3. What is AT&T's policy for responding to state law enforcement requests for call records of Vermont customers?
4. What records, if any, does AT&T keep regarding requests by law enforcement for call records of Vermont customers?

The NSA also operates a program that intercepts the contents of certain communications where one party to the communication is outside the United States and where the government has a reasonable basis to conclude that one party to the communication has a relationship with al Qaeda.³ One federal court has held that this content interception program violates the Administrative Procedures Act, the Separation of Powers Doctrine, the First and Fourteenth Amendment, and statutory law.⁴ This content interception program is not in issue here.

The Motion To Dismiss

On July 28, 2006, AT&T filed a Motion to Dismiss ("MTD") on the ground that the Board lacks subject matter jurisdiction.⁵ Fundamentally, AT&T's motion argues that the Board's jurisdiction over this matter has been preempted by federal law, "which wholly divests the states of any power to act with respect to matters of national security, national defense, and the gathering of foreign or military intelligence."⁶

3. This program was announced by President Bush and Attorney General Gonzalez in late 2004. See http://www.whitehouse.gov/news/releases/2005/12/print/20051219_1.html.

4. *American Civil Liberties Union v. National Security Agency*, ___ F.Supp. ___ slip op. at 2 (E.D. Mich., Aug. 17, 2006) (hereafter "*ACLU v. NSA*").

5. See V.R.C.P. 12(b)(1).

6. MTD at 2.

AT&T reports that this controversy may have arisen when, on May 11, 2006, the *USA Today* newspaper published a story suggesting that the NSA's intelligence-gathering activities may also have included some form of access to domestic call records databases.⁷ AT&T contends that neither the government nor AT&T has confirmed or denied the accuracy of the reports or AT&T's participation.⁸ Nevertheless, AT&T affirms that "any cooperation it affords the law enforcement or intelligence communities occurs strictly in accordance with law."⁹

AT&T reports that the United States Government ("USG") has repeatedly intervened to block lawsuits inquiring into the NSA Customer Records Program. According to AT&T, the USG "intends to assert the state secrets privilege in all of the pending actions brought and seek their dismissal."¹⁰ For example, AT&T reports that the USG filed a motion to dismiss a federal lawsuit in California, arguing that "no aspect of [the] case can be litigated without disclosing state secrets."¹¹

According to AT&T, the USG efforts have been successful, and two federal district courts have held that the NSA Customer Records Program is a state secret. In the California case ("*Hepting*"), the court barred discovery of any information relating to this claim, at least unless there are public disclosures of information relating to these allegations by the government.¹² AT&T recounts a similar result in the *Terkel* case in Illinois where the court dismissed the claims for similar reasons.

AT&T also recounts events in which the USG has acted to prevent state commissions from requiring disclosure relating to the NSA Customer Records Program. In New Jersey, the USG asserted that even disclosing whether materials exist relating to the NSA Customer Records Program "would violate various federal statutes and Executive Orders, including provisions that carry criminal sanctions."¹³ The USG also sent a similar letter to AT&T, warning AT&T that

7. See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, at A1.

8. MTD at 5.

9. MTD at 5.

10. MTD at 6.

11. MTD at 7. In that same case, the USG filed affidavits from the Director of National Intelligence ("DNI") and the Director of the National Security Agency. MTD at 8.

12. *Hepting v. AT & T Corp.*, ___ F.Supp. ___, 2006 WL 2038464 (N.D. Cal. June 20, 2006) ("*Hepting*").

13. MTD at 12 (internal quotations omitted).

""[r]esponding to the subpoenas - including by disclosing whether or to what extent any responsive materials exist - would violate federal laws and Executive Orders."¹⁴ The USG has also filed suit against utility commissioners in Missouri.¹⁵

AT&T's central argument is that this docket violates the Supremacy Clause of the United States Constitution. First, AT&T argues that this docket directly conflicts with the federal Constitution itself, because the field of foreign intelligence gathering has been fully preempted by the constitution. Requiring AT&T to answer the Department's discovery would, according to AT&T:

involve the state directly in functions that are exclusively federal: the defense of the nation against foreign attack. Under such circumstances, the state is without power to act, as these matters are regulated and controlled exclusively by federal law. Moreover . . . the questions the Department seeks responses to regarding the NSA Program cannot be answered without confirming or denying facts that are not publicly disclosed and would risk harm to the United States' efforts to protect the nation against further terrorist attack.¹⁶

AT&T also contends that states are preempted by the so-called *Totten* rule from adjudicating any matters "concerning the espionage relationships of the United States."¹⁷

Aside from constitutional considerations, AT&T also argues that Congress has enacted a variety of statutes that fully preempt this field. AT&T contends that a:

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.¹⁸

AT&T also contends that the Department's discovery requests create conflicting duties: a disclosure duty to the state; and an opposing duty to the federal government. This, AT&T argues, is a classic example of conflict preemption.

AT&T argues that when "unique federal interests" such as foreign-intelligence gathering are involved, "[t]he conflict with federal policy need not be as sharp as that which must exist for

14. MTD at 12.

15. MTD at 13.

16. MTD at 14.

17. MTD at 22, 24.

18. MTD at 28.

ordinary pre-emption when Congress legislates in a field which the States have traditionally occupied."¹⁹ This proceeding, AT&T argues, is "by its own account, 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," and is therefore entirely preempted.²⁰

AT&T also asserts that this docket calls for disclosure of information which the USG has asserted to be covered by the state secrets privilege. State secrets is a constitutionally based privilege that "protects any information whose disclosure would result in impairment of the nation's defense capabilities or disclosure of intelligence-gathering methods or capabilities."²¹ AT&T acknowledges that a state secrets claim "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," and AT&T asserts that the privilege cannot be waived by AT&T or any other private party.²² This privilege, according to AT&T, covers every aspect of this docket, "even the mere existence or non-existence of any relationship between the federal government and AT&T Corp. in connection with this program."²³

AT&T also contends that it is irrelevant that the United States has not formally invoked the state secrets privilege in this state administrative proceeding. According to AT&T, state secrets is a privilege that "is asserted in judicial proceedings where Article III judges review classified materials on an ex parte, in camera basis."²⁴ In state proceedings in New Jersey, AT&T explains that the USG did not assert the state secrets privilege, but AT&T nevertheless contends that knowing that the information has a security classification should mandate the same end.²⁵

AT&T's motion also argues that two federal statutes independently preempt the Board's jurisdiction. The first is the prohibition on disclosing "classified information . . . concerning the

19. MTD at 21-22.

20. MTD at 23.

21. MTD at 19 (internal quotations omitted).

22. MTD at 19 (internal quotations and citation omitted).

23. MTD at 20.

24. MTD at 20.

25. MTD at 21.

communication intelligence activities of the United States."²⁶ AT&T notes that the USG raised this argument in the California and Michigan cases, and elsewhere, and it contends that the risk of criminal liability prevents it from participating here.

The second statute is the National Security Agency Act of 1959. This statute says that no law may require disclosure of any information with respect to the activities of the NSA.²⁷ AT&T argues that this Board should adopt the conclusion reached by the FCC, that "the National Security Agency Act of 1959 independently prohibits disclosure of information relating to NSA activities" and that this Board lacks "authority to compel the production of the information necessary to undertake an investigation."²⁸

Participation by the United States Government

On July 31, 2006, the United States Department of Justice filed a letter on behalf of the USG ("DOJ letter"). The USG declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont."

Nevertheless, the DOJ letter takes a substantive position on the pending Motion to Dismiss. It argues generally that:

the request for information and the application of state law they embody are inconsistent with and preempted under the Supremacy Clause, and that compliance with [the Department's Document Requests], and any similar discovery propounded by the [Board], would place [AT&T] in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security.²⁹

The DOJ letter offers several legal grounds for preemption.

1. It argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.³⁰
2. It argues that providing the requested information would violate various statutes, including the National Security Agency Act and the Intelligence Reform and Terrorism

26. See 18 U.S.C. § 798.

27. See 50 U.S.C. § 402.

28. MTD at 18.

29. DOJ letter at 7.

30. DOJ letter at 3.

Prevention Act of 2004 as well as statutes and executive orders relating to classified information.³¹

3. It mentions, but does not clearly assert, the state secrets privilege. For example, the letter notes that court decisions on similar matters in another case "underscores that compliance with the requests for information would be improper."³² The closest thing to a claim of privilege in the letter is an assertion that the state secrets privilege "covers the precise subject matter sought from [AT&T] by Vermont officials."³³

The DOJ letter did not include any affidavits or sworn statement prepared for these dockets. It did include a photocopy of an affidavit submitted in a federal court proceeding by the Director of National Intelligence ("DNI") and asserting the state secrets privilege.³⁴

Responses by the Department

On August 11, 2006, the Department filed a memorandum opposing the motion. The Department argues that the petition raises matters that do not implicate national security and that, if assertions in the petition are assumed to be true, the Department would be entitled to relief.

The Department's primary contention is that the scope of this proceeding exceeds what has been arguably preempted. The Department offers a distinction between the Board investigating the privacy of AT&T's Vermont customers and AT&T's company's compliance with state and federal privacy laws, on the one hand, and on the other, the details and propriety of national security programs or the workings of the NSA.³⁵ The Department contends that the claims here "fall squarely within the Board's authority."³⁶ The scope of this proceeding, argues the Department, extends beyond AT&T's interaction with the NSA, and extends to AT&T's interactions with all state and federal agencies.³⁷

31. DOJ letter at 4-5.

32. DOJ letter at 5.

33. DOJ letter at 6.

34. DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).

35. Response at 1-2.

36. Response at 3.

37. Response at 4. On this same basis, the Department argues that AT&T's reliance on *Terkel*, is misplaced. Response at 7.

In addition, the Department apparently makes a separate argument that federal preemption has not been demonstrated here. It contends, for example, that preemption of state law is possible only where a federal agency acts within the scope of Congressionally delegated authority and makes clear its intent to preempt.³⁸

The Department concludes by recommending that the Board "allow the investigation to proceed on all claims that are not directly related to the bulk disclosure of customer calling records to the NSA."³⁹ As to interactions with the NSA, the Department recommends denying the motion for now and reviewing after the evidence is in whether the government or AT&T have by that time confirmed the existence of the program.⁴⁰

Also on August 11, the Department filed a letter responding to the DOJ letter. The letter notes that the USG has declined to intervene, and it argues that the Board should disregard the DOJ letter. The letter also argues that even where a state secrets privilege is asserted, the Board should carefully analyze whether the current circumstances warrant application of the privilege.

The letter also contends that the DOJ letter addressed only some of the issues in this docket. The Department specifically mentions AT&T's policies and practices regarding "maintaining and protecting private customer information, and whether [AT&T has] violated Vermont or federal disclosure laws, or [AT&T's] own policies."⁴¹ For example, the Department asserts that AT&T could, consistent with its asserted privilege, answer a question about whether it has:

disclosed any customer information that is deemed protected under state or federal law to any state or federal agency in the absence of a warrant, subpoena, court order or other applicable written authorization⁴²

Reading the Department's August 11 letter and August 11 memorandum together, we conclude that the Department opposes the motion on two independent grounds: (1) the scope of

38. Response at 5, citing *Global NAPS, Inc. v. AT&T New England, Inc.*, ___ F.3d ___, 2006 WL 1828612, n.7 (2d Cir. 2006).

39. Response at 8.

40. Response at 8.

41. Letter at 2.

42. Letter at 2.

this docket is broader than the materials as to which there are claims of secrecy or privilege; and (2) the claims of secrecy and privilege have not been adequately established.

AT&T's Reply

On August 18, AT&T filed a reply. Initially, AT&T clarifies that its motion was filed on the ground that the Board lacks jurisdiction over this proceeding,⁴³ not that the petition fails to state a claim on which relief can be granted.⁴⁴ AT&T argues that the Department's response, which largely addressed the latter issue, was "beside the point."⁴⁵

On substance, AT&T asserts that the Department's response "mostly seek to change the subject"⁴⁶ from federal preemption to state jurisdiction. AT&T accuses the Department of "semantic gamesmanship" in asserting that this docket is not about national security programs but about the privacy of Vermont customers.⁴⁷ The issue, AT&T maintains, is whether state regulation that otherwise would be allowable is nevertheless preempted because it interferes with foreign affairs.

AT&T contradicts the Department's assertion that the issues in this docket are broader than the NSA Customer Records Program. AT&T asserts that the Department's investigation "was inspired by, and relates directly to, the alleged participation of AT&T in communications intelligence activities of the NSA."⁴⁸ Moreover, AT&T asserts that to the extent this docket incidentally concerns disclosures to other federal agencies, inquiry into those disclosures, too, would be preempted, in part because the Board "has no power under the Constitution" to investigate such matters.⁴⁹

As noted above, the Department had argued that AT&T could properly answer a question about whether it has disclosed customer information without specific authorization by warrant or

43. See V.R.C.P. 12(b)(1).

44. See V.R.C.P. 12(b)(6).

45. Reply at 2.

46. Reply at 4.

47. *Id.*

48. Reply at 3.

49. Reply at 4.

other means. AT&T contends that an answer to this question is not sufficient to determine whether any disclosures were unlawful since:

[n]umerous provisions of federal law expressly envision that customer information might be intercepted or disclosed to government agencies without a warrant, subpoena, court order, or written authorization.⁵⁰

Finally, AT&T disagrees with the Department's recommendation that this docket be left open because of the possibility of future public disclosures. Even if such disclosures were to occur, AT&T contends this Board would still lack jurisdiction to proceed with this docket.

II. DISCUSSION

Standard for Motions to Dismiss

We consider AT&T's Motion to Dismiss as a Motion For Judgment on the Pleadings under Civil Rule 12(c).⁵¹ To grant such a motion, this Board must take as true all well-pleaded factual allegations in the petition and all reasonable inferences drawn from those allegations. We must take as false all contravening assertions in AT&T's pleadings. We may grant the motion only if the petition contains no allegations that, if proven, would permit recovery.⁵² To prevail, AT&T must show "beyond doubt that there exist no facts or circumstances that would entitle the [petitioners] to relief."⁵³

State Law - Public Service Board Jurisdiction

As a matter of state law, the Board has jurisdiction over the claims asserted in the petitions. AT&T is a company offering telecommunications services on a common carrier basis in Vermont, and it therefore is a utility subject to the Board's jurisdiction.⁵⁴ That jurisdiction extends to the manner of operating and conducting that business, so as to ensure that the service

50. Reply at 5-6.

51. AT&T's motion is stated as under Rule 12(b)(1), which established the lack of jurisdiction over the subject matter as a basis for dismissal. Construing the motion under Rule 12(c) is not incompatible with the motion. Rule 12(b) requires certain defenses to be asserted in the first responsive pleading. By applying Rule 12(c), AT&T gains the opportunity to have us consider the motion as a motion for summary judgment, and thus to consider more than the pleadings.

52. *Knight v. Rower*, 170 Vt. 96 (1999).

53. *Union Mutual Fire Ins. Co. v. Joerg*, 2003 VT 27, 4, 824 A.2d 586, 588 (2003); *Amy's Enterprises v. Sorrell*, 174 Vt. 623, 623 (2002) (mem.).

54. 30 V.S.A. § 203(5).

is reasonable and expedient, and to "promote the safety, convenience and accommodation of the public."⁵⁵ The Board has broad supervisory jurisdiction over AT&T's operations in Vermont.⁵⁶ As to matters within its jurisdiction, the Board has the same authority as a court of record.⁵⁷ In addition, the Board has authority to impose civil penalties for an improper refusal to provide information to the Department or for violating a rule of the Board.⁵⁸

The privacy of customer information has earned special mention in Vermont statutes. For example, when the Board considers a plan for alternative regulation of telecommunications companies, it must consider privacy issues.⁵⁹

The Board's authority arises solely from statute, and it does not have jurisdiction over every claim that may involve a utility. For example, the Supreme Court has held that the Board has no jurisdiction over certain traditional torts merely because the defendant is a utility.⁶⁰ AT&T's motion, however, is not based upon any such limitation in state law.

Federal Law

AT&T's central contention is that federal law preempts matters that otherwise would be within the jurisdiction of the Board under state law.⁶¹ We agree with AT&T that the supremacy clause of the United States Constitution allows federal law to preempt fully state and local laws.⁶²

It is also true, however, that this Board ordinarily applies state law until it has been demonstrably preempted. Preemption can be established in a number of ways, including explicit

55. 30 V.S.A. § 209(a)(3).

56. *In re AT&T New England, Inc.*, 173 Vt. 327, 334-35 (2002).

57. 30 V.S.A. § 9.

58. 30 V.S.A. § 30.

59. *See* 30 V.S.A. §§ 226a(c) and 226(c)(8).

60. *E.g., Trybulski v. Bellows Fall Hydro-Elect. Corp.*, 112 Vt. 1 (1941) (Board did not have jurisdiction to assess damages for injuries to private landowners' properties allegedly caused by improper maintenance and operation of dam by hydro-electric company).

61. *See, e.g., AT&T MTD* at 3, note 1 ("state agencies lack jurisdiction with respect to matters relating to AT&T's alleged cooperation with federal national security or law enforcement authorities.")

62. U.S. Const. art. VI, cl. 2; *Crosby v. National Foreign Trade Council*, 530 U.S. 363, 372, 120 S.Ct. 2288, 147 L.Ed.2d 352 (2000)

or implicit statutory language, actual conflict, or occupation of the field.⁶³ Therefore, we undertake below to evaluate each of the theories advanced by AT&T as a basis for preemption.

State Secrets

The broadest challenge to the Board's jurisdiction is that these dockets involve state secrets. The state secrets privilege contains two distinct lines of cases.

Justiciability of Claims

The first line of cases is essentially a rule of "non-justiciability" that deprives courts of authority to hear suits against the Government based on certain espionage or intelligence-related subjects. The seminal decision in this line of cases is the 1875 decision in *Totten v. United States*.⁶⁴ The plaintiff in that case brought suit against the government seeking payment for espionage services he had provided during the Civil War. The Court's decision noted the unusual nature of a contract for espionage:

The service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed. Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment, and is implied in all secret employments of the government in time of war, or upon matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties, or endanger the person or injure the character of the agent.⁶⁵

Given the unusually secret nature of these contracts, the Court held that no action was possible for their enforcement. Indeed, "[t]he publicity produced by an action would itself be a breach of a contract of that kind, and thus defeat a recovery."⁶⁶

The Supreme Court recently reaffirmed this principle in *Tenet v. Doe*.⁶⁷ In *Tenet*, the plaintiffs, who were former Cold War spies, brought estoppel and due process claims against the

63. See, e.g., *In re AT&T New England, Inc.*, 173 Vt. 327, 336 (2002).

64. 92 U.S. 105 (1875).

65. *Totten*, 92 U.S. at 106.

66. *Totten*, 92 U.S. at 107.

67. *Tenet v. Doe*, 544 U.S. 1, (2005).

United States and the Director of the Central Intelligence Agency for its alleged failure to provide them with the assistance it had allegedly promised in return for their espionage services.⁶⁸

Relying heavily on *Totten*, the Court held that the plaintiffs' claims were barred. For a unanimous Court, Chief Justice Rehnquist wrote:

We adhere to *Totten*. The state secrets privilege and the more frequent use of in camera judicial proceedings simply cannot provide the absolute protection we found necessary in enunciating the *Totten* rule. The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable. Even a small chance that some court will order disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam.'⁶⁹

The *Totten/Tenet* principle, where applicable, provides an absolute bar to any kind of judicial review, and therefore would also bar any quasi-judicial proceeding by a state agency.⁷⁰

The *Totten/Tenet* rule is inapplicable here. It applies to actions where there is a secret espionage relationship between the Plaintiff and the Government.⁷¹ Petitioners here do not claim to be spies or to have any form of secret espionage relationship with the government. Therefore the absolute bar rule does not apply to these dockets.

Evidentiary Privilege

The second branch of the State secrets doctrine deals with the exclusion of evidence, and the consequences of that exclusion.

The effect of the state secrets privilege on plaintiffs is like other evidentiary privileges. Where a privilege blocks admission of some evidence, a plaintiff nevertheless may use other evidence to prove his or her case. However, if the plaintiff fails to carry its burden of proof, the court may dismiss the case or grant summary judgment against the plaintiff, as in any other proceeding.⁷²

68. *Tenet* at 3.

69. *Tenet* at 11 (citations omitted).

70. *Tenet* at 8.

71. *Tenet* at 7-8; *ACLU v. NSA* at 10-11; cf. *Terkelat* 15-16 (declining to extend *Totten* principle to disclosure of telephone records to the government because such disclosures are not inherently harmful to national security and would reveal violations of plaintiffs' statutory rights).

72. *United States v. Reynolds*, 345 U.S. 1, 11 (1953); *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C.Cir. 1983).

For defendants, the state secrets privilege produces the opposite of the normal result. Normally a defendant who needs privileged evidence admitted into evidence is harmed by the privilege. With the state secrets privilege, however, the defendant gains an advantage. Where a defendant needs evidence comprising a state secret in order to create a valid defense, summary judgment must be granted to the defendant.⁷³

For two independent reasons, we deny the Motion to Dismiss on grounds of the state secrets privilege.

1. AT&T has not properly invoked the privilege

The United States Supreme Court has explained that the state secrets "privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party. Moreover, there must be a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer."⁷⁴

Here, the government has declined to become a party, despite our earlier invitation to do so.⁷⁵ AT&T is a party, but under federal law it does not have standing to raise the privilege. Moreover, no party has submitted any sworn statement prepared for these dockets. Instead, both AT&T and the DOJ letter included photocopies of affidavits filed in other proceedings by the Director of National Intelligence.⁷⁶

A motion to dismiss may be treated as a motion for summary judgment if it involves matters outside the pleadings.⁷⁷ Since the DOJ letter is not a pleading, we could grant summary judgment for AT&T if the record shows that there are no material facts that are genuinely in

73. *Kasza*, 133 F.3d at 1166; *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992). Normally a defendant relying on privileged evidence would be deprived of that evidence, and might thereby lose a valid defense. However, by requiring dismissal in such cases, the state secrets privilege uniquely operates to benefit defendants in all cases, regardless of which party needs the secret evidence.

74. *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Hepting* at 16.

75. As noted above, the Department of Justice declined to intervene and asserted that its letter should not be deemed to be a "submission of the United States to the jurisdiction of Vermont." We are puzzled by this statement because we are not aware that when the United States intervenes in a state administrative proceeding the form gains "jurisdiction" over the federal government.

76. *E.g.*, DOJ letter, attachments from July 28 FAX at 16-17 (Negroponte statement at 4-5).

77. V.R.C.P. 12(c).

dispute. Partial summary judgment can also be granted when only some issues are in dispute.⁷⁸ Summary judgment can be granted without affidavits,⁷⁹ but affidavits can be used to show that no material issue of fact exists. Where affidavits are submitted, they must be based upon personal knowledge.⁸⁰

We noted above that federal law requires the government to claim the state secrets privilege. This is not an empty formality. Because the privilege, once accepted, creates an absolute bar to the consideration of evidence, the courts do not lightly accept a claim of privilege. In each case, the government's showing of necessity for the privilege determines "how far the court probes in satisfying itself that the occasion for invoking the privilege is appropriate."⁸¹ The courts have made it clear that "control over the evidence in a case cannot be abdicated to the caprice of executive officers."⁸² The privilege may not be used to shield any material not strictly necessary to prevent injury to national security; and, whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.⁸³

Federal courts have frequently conducted *in camera* proceedings to test the assertion of the privilege.⁸⁴ In the recent *Terkel* case, the government has voluntarily filed both public and secret *in camera* affidavits for the courts' consideration.⁸⁵ We recognize that *in camera* proceedings before this Board may present difficulties that do not arise in federal courts. However, we understand the relevant federal law to require not only that the privilege be claimed by the responsible official but that the trier of fact at least minimally test whether "the occasion for invoking the privilege is appropriate."⁸⁶ We are not convinced that those difficulties cannot be overcome.⁸⁷

78. V.R.C.P. 12(d). Summary judgment cannot be granted, however, without offering the parties a reasonable opportunity to present material pertinent to the motion. V.R.C.P. 12(c).

79. V.R.C.P. 56(b).

80. V.R.C.P. 56(e); *Department of Social Welfare v. Berlin Development Assoc.*, 138 Vt. 160 (1980).

81. *U.S. v. Reynolds*, 345 U.S. at 11.

82. *U.S. v. Reynolds*, 345 U.S. at 11.

83. *Ellsberg v. Mitchell*, 709 F.2d 51, 56 (D.C. Cir. 1983).

84. *E.g.*, *Hepting* at 4; *Terkelat* 5, 21.

85. *Terkelat* 5. The DOJ letter here attached a photocopy of the affidavit from *Terkel*.

86. *U.S. v. Reynolds* at 11.

87. See discussion below of CIPA rules for sharing of classified information in "graymail" cases.

The privacy issues raised in these dockets are of great interest to Vermont ratepayers, and we are not willing to dismiss this proceeding without, at minimum, affidavits sufficient to justify that action. Therefore we hold that the government's claim of privilege must be accompanied by at least some admissible evidence, ordinarily by affidavit, from a responsible official who asserts after personal consideration that the subject matter is a state secret.⁸⁸ No such affidavit has been submitted in this proceeding. Therefore the state secrets privilege has not been properly claimed here.

2. The state secrets privilege, if it did apply, would not bar all pending claims.

If the Department cannot prove that AT&T has participated in the NSA Customer Records Program, it may still be entitled to some relief here. For example, the Department may request the Board to order AT&T to modify its existing customer privacy notices to describe the policies that AT&T would apply in the *hypothetical* event that AT&T is asked in the future to disclose confidential customer information pursuant to a secret government program. Even if this Board cannot consider what *has* happened, we are not preempted from requiring AT&T to provide notice to customers describing how AT&T would apply the known structures of federal law to government requests for otherwise private information.⁸⁹

As noted above, AT&T has asserted that "any cooperation it affords the law enforcement or intelligence communities occurs strictly in accordance with law."⁹⁰ AT&T also asserts, however, that "[n]umerous provisions of federal law expressly envision that customer information might be intercepted or disclosed to government agencies without a warrant, subpoena, court order, or written authorization."⁹¹ The Department may legitimately seek more information regarding AT&T's beliefs about the circumstances under which the law allows such interception and disclosure. In particular, the Department may want to know more about the circumstances under which AT&T believes that it may disclose customer information without

88. See, e.g., *Hepting* at 16 (state secret privilege requires a formal claim by agency head after personal consideration).

89. This point is underscored by the breadth of the claims in AT&T's filings and in the DOJ letter. Those documents demonstrate that, regardless of what AT&T has done in the past, if it were to agree in the future to provide the NSA with customer record information, AT&T would consider itself barred from disclosing that fact.

90. MTD at 5.

91. Reply at 5-6.

warrants, written findings or other documents. These facts also might appropriately influence the content of customer notices and the company's written privacy policies.

Field Preemption

AT&T and the USG argues that providing the requested information would interfere with the Nation's foreign-intelligence gathering, a field reserved exclusively to the Federal Government.⁹² They argue: (1) the field of foreign-intelligence gathering has been fully preempted; and (2) this prevents any and all state inquiry into communications between AT&T and the NSA that USG describes as part of the USG's foreign-intelligence gathering efforts. While the first proposition above may be true, the second requires proof.

We reject the field preemption argument for procedural reasons. As we noted above, the USG has not appeared in this proceeding and has not offered any sworn evidence supporting its position. Instead, it has provided photocopies of affidavits it submitted in other proceedings. It is not enough, as the USG asserts, that a high government official recently told a federal court in another state that this subject involves national security.

AT&T also argues that federal legislation preempts the field, which it defines as "the cooperation of telecommunications carriers with the federal government's intelligence-gathering and surveillance activities."⁹³ AT&T cites the Communications Assistance to Law Enforcement Act ("CALEA"),⁹⁴ the Wiretap Act,⁹⁵ the Stored Communications Act,⁹⁶ and the Foreign Intelligence Surveillance Act (FISA).⁹⁷ AT&T concludes that this complex federal scheme leaves no room for state regulation of an exclusively federal function.

We reject this statutory argument. It is true that a variety of federal statutes exist that regulate the relationship between telecommunications carriers and federal police agencies. While many aspects of the relationship between telecommunications carriers and police have indeed been so defined, AT&T fails to show that this fully preempts the field. For example, states differ

92. DOJ letter at 3.

93. MTD at 28.

94. See 47 U.S.C. § 1001 *et seq.*

95. See 18 U.S.C. § 2511 *et seq.*

96. See 18 U.S.C. § 2701 *et seq.*

97. See 50 U.S.C. § 1804(a)(4); 50 U.S.C. § 1805(c)(2).

among themselves regarding the requirements for wiretap warrants. If the relationship between police agencies and telecommunications carriers can vary by state, the field has not been preempted by comprehensive Congressional enactments.

Statutory Arguments

The NSA Statute

AT&T and the DOJ letter assert that Section 6(a) of the National Security Agency Act of 1959 ("NSA Statute") requires dismissal. This statute provides:

Sec. 6. (a) . . . [N]othing 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 the persons employed by such agency.⁹⁸

On its face, this statute is extraordinarily broad. By its terms, it trumps *any* "other law," state or federal. One federal court, commenting on the breadth of this statute observed that if this statute were:

taken to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions.⁹⁹

Courts have nevertheless applied the statute as written. For example, the statute gives the NSA the absolute right to resist a Freedom of Information request seeking disclosure of information from the NSA's own files regarding its own operations.¹⁰⁰

AT&T's interpretation would further expand the reach of the statute. AT&T argues: (1) it may have provided information to the NSA; and (2) requiring it to now explain what it did would improperly disclose the activities of the NSA.

This interpretation not only protects NSA employees, officers and files from forced disclosures, but it would also apply the statute to people with whom the NSA has had contact and from whom it has requested information. The argument seems to be a form of "Midas Touch" for the NSA: anything it touches becomes secret. Once the USG has asserted that the activities

98. Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note.

99. *Terkelat* 11.

100. *Id.*; *Hayden v. National Security Agency*, 608 F.2d 1381 (D.C. Cir. 1979).

of *any* private person also relate to NSA activities, the USG's argument seems to require that the activity as a whole becomes privileged and all state inquiry about that activity must cease, regardless of the consequences to petitioners, respondents, utilities and customers. This goes far beyond the scope of a statute nominally aimed at keeping confidential the names, salaries and activities of NSA employees. Moreover, courts have made clear that a simple assertion that Section 6(a) applies is inadequate. For example, in *Founding Church of Scientology v. NSA*, the Court of Appeals for the District of Columbia rejected the District Court's reliance upon an affidavit from the NSA invoking Section 6 when that affidavit made simple conclusory assertions which were not substantiated.¹⁰¹ Here, AT&T has simply made broad assertions, unsupported by an affidavit by the NSA. Therefore, we conclude that AT&T has not presented a sufficiently detailed basis for us to find that Section 6(a) bars disclosure of all information that may be relevant to this proceeding.

Even though the courts have applied Section 6(a) broadly, for an independent reason it does not support dismissal at this time. In the *Hepting* case in Northern California, Judge Walker denied dismissal of similar claims, even though he blocked discovery on those same claims. He noted the possibility that the government or the defendant telecommunications carrier might make public disclosures that would support the claims made in that case. Instead of dismissing the case, the judge offered to make step-by-step determinations during discovery as to whether the various privileges would prevent plaintiffs from discovering evidence.¹⁰²

We have decided to follow the same course. AT&T or other utilities who participated in the NSA Customer Records Program may make further disclosures that are sufficiently reliable to alter the outcome. Although some of the petitioner's discovery requests may be blocked by one or another privilege, some information about AT&T's activities may nevertheless emerge. Later, AT&T might be entitled to summary judgment if the state secrets privilege blocks certain items of evidence that are essential to plaintiffs' prima facie case or to AT&T's defense. Alternatively, time may provide petitioners more non-classified and admissible materials, and it is at least conceivable that some of petitioner's claims could survive summary judgment. As

101. 610 F.2d 824, 831-833 (1978).

102. *Hepting* at 21.

discovery proceeds, we will be willing to determine step-by-step whether the privilege prevents petitioner from discovering particular evidence. The mere existence of the NSA statute, however, does not justify dismissing this docket now.

Foreign Intelligence Surveillance Act

The DOJ letter asserts that AT&T may not provide information by a provision of the Foreign Intelligence Surveillance Act ("FISA"). These statutes relate to the terms of judicial FISA orders authorizing electronic surveillance. They allow a court issuing a surveillance warrant to direct a common carrier to cooperate in executing that warrant and also to direct that the carrier protect the secrecy of the surveillance while minimally interfering with the target's normal services.¹⁰³ The statutes also allow the court to require the carrier to keep records of the surveillance.¹⁰⁴

These statutes are irrelevant. Nothing in the record suggests that AT&T ever received a FISA warrant regarding the NSA Customer Records Program.

As noted above, the federal government operates a program of warrantless interception of certain communications involving persons suspected of having contacts with al Qaeda has recently been reviewed in the courts. One court has held that this program violates FISA because the program "has undisputedly been implemented without regard to FISA."¹⁰⁵ If the United States government operates its content interception program without recourse to FISA, we see little reason to infer that it would use those procedures to obtain disclosure of telecommunications records.

Classified Information

AT&T also moves to dismiss on the grounds that if it has participated in the NSA Customer Records Program, that program, and AT&T's participation, would be classified information. As a result, if AT&T were required to provide such information it would be

103. 50 U.S.C. § 1805(c)(2)(B).

104. 50 U.S.C. § 1805(c)(2)(C).

105. *ACLU v. NSA* at 2.

subject to prosecution for a felony.¹⁰⁶ Therefore, AT&T argues that the federal classification imposes conflicting state and federal duties, in which the federal duty must be supreme.

The DOJ letter asserts that various Executive Orders require that classified information cannot be disclosed unless the head of the agency imposing the classification has authorized disclosure, the recipient has signed a nondisclosure agreement, and the person has a need-to-know.¹⁰⁷ According to the DOJ, Vermont state officials do not qualify.

Initially, we note that the DOJ letter suggests that a very broad category of information is classified. The DOJ letter asserts the claim for any and all matters relating to the "foreign-intelligence activities of the United States."¹⁰⁸ Given the context, however, this also includes domestic data collection activities. In this sense, the USG defines "foreign-intelligence" by the purpose of the activity, not the location at which the information is collected.

We also note that this dispute does not involve a party seeking disclosure of information held in government files or a party seeking to compel the testimony of a government official or employee. Instead, the alleged classified activity involves the activities of civilian employees of a telecommunications company regulated in Vermont. The petitioners assert that AT&T may have transferred data to the government or even given the government access to customer information and calling patterns contained in the utility's files. Therefore what is putatively classified here is the knowledge of AT&T's officials and employees, and that knowledge may consist of nothing more than network design information or software access information.

"Graymail" is a practice by criminal defendants in which the defendant seeks to avoid prosecution by threatening to disclose classified materials in open court.¹⁰⁹ Congress enacted a statute to deal with this problem, the Classified Information Procedures Act (CIPA).¹¹⁰ Under CIPA, when it appears that classified information may be disclosed in a criminal case, any party may move for a pretrial conference to consider rules for discovery and disclosure of that

106. 18 U.S.C. § 798(a)(1) prohibits making available to an unauthorized person any "classified information" relating to the "communications intelligence activities of the United States."

107. DOJ letter filed 7/31/06 at 4-5.

108. DOJ letter at 5.

109. In these cases the USG is often already a party.

110. 18 U.S.C.A. App. §§ 1-16.

information.¹¹¹ A defendant may not disclose classified information at trial without giving advance notice to the Attorney General,¹¹² who can then request a hearing to protect the information.¹¹³ The court must conduct a hearing if one is requested, and the hearing may be held *in camera*.¹¹⁴ Where a defendant seeks and ultimately receives classified information, the court can enter an order preventing further disclosure.¹¹⁵ When the Attorney General submits an affidavit certifying that information is classified, the court may authorize the government to submit redacted documents, to submit summaries of documents, or to admit relevant facts.¹¹⁶

Under CIPA, court personnel have access to classified information. To facilitate this process, the Chief Justice of the United States has determined that no security clearances are required for judges, and security clearances have been sought for other court personnel.¹¹⁷ The government can even compel defense counsel to undergo a DOJ initiated security clearance procedure,¹¹⁸ and classified information can be provided to the defendant's counsel.¹¹⁹

Like CIPA, these dockets present a conflict between a party's rights (and need for evidence to exert those rights) and the government's need to keep the information from disclosure because of its potential harm to national security interests.¹²⁰ We find it instructive that CIPA allows a criminal court wide latitude to balance these interests and to use tools such as security clearances, closed hearings, redaction, summaries and protective orders. We also find it instructive that the government in CIPA cases has offered (and even mandated) security clearances for criminal defense counsel. It is disappointing that the USG has not offered to use any such limiting techniques in this proceeding. Nevertheless, CIPA does not apply here. While we might wish the law were otherwise, we have no legal authority to insist upon CIPA-like

111. See 18 U.S.C.A. App. § 2.

112. See 18 U.S.C.A. App. § 5(a).

113. See 18 U.S.C.A. App. § 6(a).

114. See 18 U.S.C.A. App. § 6(a).

115. See 18 U.S.C.A. App. § 3.

116. See 18 U.S.C.A. App. § 6(c)(2).

117. *U.S. v. Jolliff*, 548 F.Supp. 229, 231 (D. Md. 1981).

118. *U.S. v. Bin Laden*, 58 F.Supp.2d 113 (S.D.N.Y. 1999).

119. *Jolliff, Bin Laden*, above.

120. CIPA also involves other constitutional rights such as the right to assistance of counsel and the right to confront adverse witnesses in criminal cases.

procedures. Yet, it is hard to understand why criminal defendants' rights to life and liberty are more important than an alleged infringement of thousands of Vermont citizens' right to privacy.

The issue here, therefore, is whether we should deny relief to the petitioner in this proceeding because the petition seeks information that may be classified. In deciding this question, we return again to the key fact that there is no sworn evidence or affidavits on any of these matters. We conclude that there is no evidentiary basis to find that federal classification systems will prevent us from reaching a decision in this matter. Unlike CIPA cases in which the government must present an affidavit opposing release of classified information, here we have only a letter and a photocopy of an affidavit submitted elsewhere. This does not provide an adequate basis to dismiss the petition.

In addition, as we did above, we rely on the possibility of future disclosures. As the *Hepting* court found, reliable public disclosures between now and the time that this case is decided may allow petitioner to establish a right to relief independent of classified information.

Intelligence Reform and Terrorism Prevention Act of 2004

The USG asserts that requiring AT&T to reply to discovery in this docket would violate the Intelligence Reform and Terrorism Prevention Act of 2004.¹²¹ This statute gives the Director of National Intelligence ("DNI") the authority to "protect intelligence sources and methods from unauthorized disclosure."¹²²

This statute is clear on its face. It imposes a duty on the DNI, not on this Board. One might argue that this statute obligates the DNI to intervene in these proceedings to protect intelligence sources. It might even be arguable that this statute gives the DNI a defense to an action seeking disclosure of information he holds. The statute clearly does not, however, create a duty for this Board to dismiss dockets brought by customers and the Department against a utility.¹²³ It certainly does not require us to do so without receiving evidence that draws a connection between the evidence sought and the sworn evidence that this intrudes upon the government's intelligence sources and methods.

121. DOJ letter at 4.

122. Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1).

123. *Terkel*, slip op. at 12.

III. CONCLUSION

We deny AT&T's Motion to Dismiss because we have jurisdiction under state law to proceed in this matter, and it has not been shown that federal law preempts that jurisdiction. Moreover, we conclude that there is the possibility that facts will be adduced to sustain petitioners' claims. We recognize that the Department may now seek discovery of a sort recently prohibited by two federal district courts. However, we believe that the better approach is to limit discovery on a more particularized basis.

SO ORDERED.

Dated at Montpelier, Vermont, this 18th day of September, 2006.

<u>s/ James Volz</u>)	
)	
)	PUBLIC SERVICE
)	
<u>s/ David C. Coen</u>)	BOARD
)	
)	OF VERMONT
)	
<u>s/ John D. Burke</u>)	

OFFICE OF THE CLERK

FILED: September 18, 2006

ATTEST: s/ Susan M. Hudson
Clerk of the Board

NOTICE TO READERS: This decision is subject to revision of technical errors. Readers are requested to notify the Clerk of the Board (by e-mail, telephone, or in writing) of any apparent errors, in order that any necessary corrections may be made. (E-mail address: psb.clerk@state.vt.us)



COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
P.O. BOX 3265, HARRISBURG, PA 17105-3265

ISSUED: August 18, 2006

IN REPLY PLEASE
REFER TO OUR FILE
C-20066397 et al

KENNETH I TRUJILLO ESQUIRE
KATHRYN C HARR ESQUIRE
TRUJILLO RODRIGUEZ & RICHARDS LLC
THE PENTHOUSE
226 RITTENHOUSE SQUARE
PHILADELPHIA PA 19103

ACLU of Pennsylvania, et al.
v.
AT&T Communications of PA, LLC, et al.

TO WHOM IT MAY CONCERN:

Enclosed is a copy of the Initial Decision of Administrative Law Judge Charles E. Rainey, Jr. This decision is being issued and mailed to all parties on the above specified date.

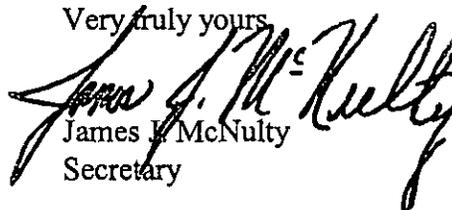
If you do not agree with any part of this decision, you may send written comments (called Exceptions) to the Commission. Specifically, an original and nine (9) copies of your signed exceptions **MUST BE FILED WITH THE SECRETARY OF THE COMMISSION 2ND FLOOR KEYSTONE BUILDING, NORTH STREET, HARRISBURG, PA OR MAILED TO P.O. BOX 3265, HARRISBURG, PA 17105-3265**, within twenty (20) days of the issuance date of this letter. The signed exceptions will be deemed filed on the date actually received by the Secretary of the Commission or on the date deposited in the mail as shown on U.S. Postal Service Form 3817 certificate of mailing attached to the cover of the original document (52 Pa. Code §1.11(a)) or on the date deposited with an overnight express package delivery service (52 Pa. Code 1.11(a)(2), (b)). If your exceptions are sent by mail, please use the address shown at the top of this letter. A copy of your exceptions must also be served on each party of record. 52 Pa. Code §1.56(b) cannot be used to extend the prescribed period for the filing of exceptions/reply exceptions. A certificate of service shall be attached to the filed exceptions.

If you receive exceptions from other parties, you may submit written replies to those exceptions in the manner described above within ten (10) days of the date that the exceptions are due.

Exceptions and reply exceptions shall obey 52 Pa. Code 5.533 and 5.535 particularly the 40-page limit for exceptions and the 25-page limit for replies to exceptions. Exceptions should clearly be labeled as "EXCEPTIONS OF (name of party) - (protestant, complainant, staff, etc.)".

If no exceptions are received within twenty (20) days, the decision of the Administrative Law Judge may become final without further Commission action. You will receive written notification if this occurs.

Very truly yours,


James E. McNulty
Secretary

Encls.
Certified Mail
Receipt Requested
jeh

**BEFORE THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION**

ACLU of Pennsylvania, et al.	:	
	:	
v.	:	C-20066397
	:	
AT&T Communications of PA LLC	:	
	:	
ACLU of Pennsylvania, et al.	:	
	:	
v.	:	C-20066398
	:	
Verizon Pennsylvania Inc.	:	
	:	
ACLU of Pennsylvania, et al.	:	
	:	
v.	:	C-20066399
	:	
Verizon North Incorporated	:	
	:	
ACLU of Pennsylvania, et al.	:	
	:	
v.	:	C-20066401
	:	
CTSI, LLC	:	
	:	
ACLU of Pennsylvania, et al.	:	
	:	
v.	:	C-20066404
	:	
ARC Networks Inc.	:	
	:	
CWA District 13/Terrance T. Tipping	:	
	:	
v.	:	C-20066410
	:	
Verizon Pennsylvania Inc.	:	
	:	
CWA District 13/Terrance T. Tipping	:	
	:	
v.	:	C-20066411
	:	
Verizon North Incorporated	:	

CWA District 13/Terrance T. Tipping	:	
	:	
v.	:	C-20066412
	:	
Verizon Select Services Inc.	:	
	:	
CWA District 13/Terrance T. Tipping	:	
	:	
v.	:	C-20066413
	:	
AT&T Communications of PA LLC	:	

INITIAL DECISION

Before
Charles E. Rainey, Jr.
Administrative Law Judge

HISTORY OF THE PROCEEDING

I. **ACLU Complaints**

On May 24, 2006, American Civil Liberties Union of Pennsylvania, Pennsylvania Coalition Against Domestic Violence, HAVIN, Inc., William Way Community Center, AIDS Community Alliance of South Central PA, Common Roads, Alyce Bowers, Katherine Franco, Lynne French, Louis M. Gehosky, David M. Jacobson, Rev. Robin Jarrell, Stephanie Parke, Marie Poulsen, Gregory Stewart, Barbara Sutherland, Francis Walsh, Michael Wolf and John Wolff (collectively referred to herein as "ACLU") filed a formal complaint against AT&T Communications of Pennsylvania (AT&T), Verizon Pennsylvania Inc. and Verizon North Inc. (collectively referred to herein as "Verizon"), CTSI, LLC (CTSI) and ARC Networks Inc. d/b/a InfoHighway Communications (InfoHighway)¹ with the Pennsylvania Public Utility

¹ ACLU's complaint was also filed against United Telephone Company of Pennsylvania d/b/a Embarq Pennsylvania (C-20066400), Denver & Ephrata Telephone & Telegraph Company (C-20066402) and Buffalo Valley Telephone Company (C-20066403). However, by letters filed July 12, 2006, ACLU withdrew the complaint against Denver & Ephrata Telephone Company and Buffalo Valley Telephone Company. And by letter filed July 17, 2006, ACLU withdrew the complaint against United Telephone Company of Pennsylvania. The Commission treated the letters as petitions for leave to withdraw the complaint as to those respondents, and when no timely objections were filed, the Commission closed the cases as to those respondents.

Commission (Commission) pursuant to 52 Pa. Code §§5.21(Formal complaints generally) and 63.135 (Customer information)². ACLU alleges that it believes that respondents violated 52 Pa. Code §63.135 by voluntarily disclosing to the National Security Agency (NSA) (without requiring the production of a search warrant or court order), the personal calling patterns of millions of Pennsylvania telephone customers, including telephone numbers called, and the time, date and direction of calls. The Commission's Secretary's Bureau divided the complaint into separate complaints against each of the named telecommunications carriers, and assigned each complaint a separate docket number. The Commission's Secretary's Bureau then served a copy of the complaint on each of the named respondents. See, 66 Pa.C.S. §702 (Service of complaints on parties).

On June 20, 2006, AT&T filed an answer and preliminary objection in the nature of a motion to dismiss the complaint at docket number C-20066397. On June 21, 2006, AT&T filed an affidavit as a supplement to its answer.

On June 20, 2006, Verizon filed in regard to the complaints at docket numbers C-20066398 and C-20066399, preliminary objections and a "response".

On June 20, 2006, CTSI filed at docket number C-20066401 an answer and "new matter directed to complainants" and "new matter directed to co-respondents".

Filed at docket number C-20066404 on June 21, 2006, is a letter in lieu of an answer, authored by Jeffrey E. Ginsberg, the Chairman of InfoHighway.

On June 26, 2006, ACLU filed a letter requesting a 10-day extension of time to file responses to the motions of AT&T and Verizon.³ On June 26, 2006, ACLU filed a letter stating that AT&T had no objection to its request. By Notice dated June 27, 2006, the parties

² In the complaint, ACLU actually refers to these Sections as being under the Public Utility Code. However, they are not. The Public Utility Code provides the Commission's statutory authority, and those statutes are found under Title 66 of the Pennsylvania Consolidated Statutes. The Sections referenced by ACLU are Commission regulations found under Title 52 of the Pennsylvania Code.

³ ACLU's letter also requested an extension of time to respond to preliminary objections filed by Denver & Ephrata Telephone & Telegraph Company and Buffalo Valley Telephone Company. However, as previously noted, ACLU subsequently withdrew its complaint as to those companies.

were informed that ACLU's request for an extension of time was granted and that answers to the motions were required to be filed on or before July 17, 2006. On July 14, 2006, ACLU filed responses to the motions.

On August 2, 2006, AT&T filed a "Supplement" to its motion to dismiss the complaint at docket number C-20066397.

II. CWA Complaints

On May 24, 2006, District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, (collectively referred to herein as "CWA") filed formal complaints against Verizon (including Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc.) (C-20066410, C-20066411 and C-20066412) and AT&T (C-20066413). CWA alleges that Verizon and AT&T possibly engaged in "unreasonable utility practices" if they participated in "the NSA's domestic wiretapping program." The Commission's Secretary's Bureau served copies of the complaints on the appropriate respondents.

On June 20, 2006, Verizon filed in regard to the complaints at docket numbers C-20066410, C-20066411 and C-20066412, preliminary objections and a "response".

Also on June 20, 2006, Verizon filed at the aforementioned docket numbers, a motion for the admission *pro hac vice* of Leigh A. Hyer, Esquire. No timely objections to the motion for admission *pro hac vice* were filed. Verizon's motion for the admission *pro hac vice* of Leigh A. Hyer, Esquire is granted.

On June 22, 2006, AT&T filed an answer and preliminary objection in the nature of a motion to dismiss CWA's complaint at docket number C-20066413.

CWA did not file a timely answer or response to either the preliminary objections of Verizon or the preliminary objection in the nature of a motion to dismiss of AT&T. I also note that CWA did not file a request for an extension of time to file an answer or response.

III. Consolidation of complaints

Commission rules provide in pertinent part:

§5.81 Consolidation.

(a) The Commission or presiding officer, with or without motion, may order proceedings involving a common question of law or fact to be consolidated. The Commission or presiding officer may make orders concerning the conduct of the proceeding as may avoid unnecessary costs or delay.

52 Pa. Code §5.81(a). The ACLU and CWA complaints involve common questions of law and fact. I am therefore consolidating the ACLU and CWA complaints for the purpose of adjudicating this matter.

DISCUSSION

The basis of ACLU's complaint is principally an article that appeared in *USA Today* on May 11, 2006, as well as articles that appeared shortly thereafter in the *New York Times* and *Wall Street Journal*. Complaint at 8-10, 12. Based on those articles, ACLU alleges that it believes that since September 11, 2001, AT&T and Verizon violated 52 Pa. Code §63.135 by voluntarily disclosing to the NSA, (and not requiring it to produce a search warrant or court order), the personal calling patterns of millions of Pennsylvania customers, including telephone numbers called, time, date and direction of calls. *Id.* at 2, 9, 13. ACLU also alleges that it "reasonably believe[s]" that the other respondents named in its complaint have and are committing the same violation. *Id.* at 13. ACLU further alleges that with the information provided by respondents, the NSA "can easily determine the names and addresses associated with these calls by cross-referencing other readily available databases." *Id.* at 2, 9. ACLU requests that the Commission order respondents to: (1) provide ACLU and the Commission with a complete accounting of any and all releases of customer information to the NSA or any other

federal or state law enforcement agency⁴ that was not compelled by court order or warrant; (2) cease and desist from releasing customer calling information to the NSA or other law enforcement agencies without court order or warrant; and (3) take such steps as are necessary to comply with Pennsylvania law. Id. at 14. ACLU also seeks “such other relief as the Commission may deem necessary and proper.” Id. at 14.

CWA indicates that its complaints are based on “official statements and press releases” regarding “the NSA’s domestic wiretapping program.” CWA alleges that Verizon and AT&T possibly engaged in “unreasonable utility practices” if they participated in the NSA’s domestic wiretapping program. CWA requests that the Commission investigate whether respondents are “cooperating in Pennsylvania, with the National Security Agency’s (NSA) warrantless domestic wiretapping program.” Specifically, CWA requests that the Commission “use its statutory authority” to compel respondents to answer four questions. Those four questions are:

1. [Have respondents] provided NSA with unwarranted access to call records, e-mail records and unwarranted access to [respondents’] facilities in Pennsylvania?⁵
2. [Have respondents] allowed the NSA to tap calls and read e-mails of [respondents’] customers in Pennsylvania?
3. [Have respondents] provided data mining samples of telephone calls and e-mails to NSA?
4. [Have respondents] allowed telephone and e-mail data to be directly sampled by NSA?

See, attachments to CWA’s completed formal complaint forms.

In its preliminary objection in the nature of a motion to dismiss the complaints of ACLU and CWA, AT&T argues that the Commission lacks jurisdiction to hear the complaints.

⁴ My references in this Initial Decision to “the NSA” includes any other law enforcement and governmental agencies which complainants allege may have received customer calling information from respondents.

⁵ The question marks after the questions were supplied. In the attachments to the complaints, the questions were punctuated with periods.

AT&T asserts that at the core of complainants' complaints are significant legal issues governed exclusively by federal law which divests the states of any power to act. AT&T Motion at 1-2. Those significant legal issues according to AT&T are: (1) the scope of authority of the Executive Branch of the United States government to conduct intelligence-gathering activities in furtherance of national security; and (2) the ability of the United States to protect classified information. Id. at 1.

AT&T asserts that at least two federal statutes, 18 U.S.C. §798 and 50 U.S.C. §402 (§6 of the National Security Agency Act of 1959), preempt proceedings before the Commission on the complaints. Id. at 10. AT&T notes that 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. at 11. And AT&T notes that §6 of the National Security Agency Act (“the Act”) prohibits the disclosure of any information regarding the activities of the NSA. Id. at 12. 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. Id. at 12.

AT&T emphasizes that “[t]he 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.” Id. at 11. AT&T avers that the United States Department of Justice sent it a letter dated June 14, 2006, warning it that “responding to subpoenas [issued by the New Jersey Attorney General] – including by disclosing whether or to what extent any responsive materials exist – would violate federal laws and Executive Orders.” Id. at 8. AT&T argues that therefore it would violate federal criminal statutes if it participated in any state investigation, as it would be required, at a minimum, to disclose whether it was in possession of relevant information. Id. at 12.

AT&T points out that the Federal Communications Commission (FCC) declined to undertake an investigation after it determined that any investigation would require the

production of classified information relating to NSA activities, and that it, the FCC, lacks the authority to compel the production of classified information. Id. at 13. AT&T opines that the Commission should make the same determination in regard to the present complaints. Id.

AT&T argues that a Commission investigation into the complaints of ACLU and CWA is also barred by the state secrets privilege, the Totten rule, the Communication Assistance to Law Enforcement Act (CALEA) and the Foreign Intelligence Act (FISA). Citing Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983), AT&T explains that “[t]he state secrets privilege is a constitutionally-based privilege belonging exclusively to the federal government that protects any information whose disclosure would result in impairment of the nation’s defense capabilities.” AT&T Motion at 14. The Totten rule, according to AT&T, 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). Id. at 17. And AT&T states that CALEA, 47 U.S.C. §1001 et seq., provides at §1002(a) 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.” Id. at 19. AT&T also explains that 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.” 50 U.S.C. §§1804(a)(4) and 1805(c)(2). Id. at 21. AT&T also reminds us that the Commission does not have jurisdiction under the Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S. §§5701-5781, to determine the legality of electronic surveillance. McClellan v. PUC, 634 A.2d 686, 159 Pa. Commw. 675 (1993). Id. at 22-23. Such jurisdiction rests in the court of common pleas, asserts AT&T. Id.

Verizon in its preliminary objections argues that the complaints of ACLU and CWA should be rejected because they: (1) request relief beyond the Commission’s authority to grant; and (2) are legally insufficient. Verizon P.O. at 1. In support of its preliminary objections Verizon, like AT&T, point to the FCC’s refusal to investigate the alleged violations due to the classified nature of the NSA’s activities. Id. at 2. Verizon also notes that it (like AT&T) was

sent a letter by the United States Department of Justice warning it that responding to the New Jersey Attorney General's subpoena "would be inconsistent with and preempted by federal law." Id. at 2-3. Consequently, according to Verizon, because national security is implicated, the Commission will be unable to adduce any facts relating to the claims of ACLU and CWA and thus will be unable to resolve the issues raised in the requests of ACLU and CWA. Id. at 3.

Verizon admits that it "cooperates with national security and law enforcement requests within the bounds of the law." Id. at 6. It argues that "[t]he Wiretap Act, FISA, the Electronic Communications Privacy Act, and the Telecommunications Act all contain exceptions to the general prohibitions against disclosure and expressly authorize disclosure to or cooperation with the government in a variety of circumstances." Id. at 7 (footnote omitted). Verizon also argues that "these laws provide that 'no cause of action shall lie' against those providing assistance pursuant to these authorizations, and also that 'good faith reliance' on statutory authorizations, court orders, and other specified items constitutes 'a complete defense against any civil or criminal action brought under this chapter or any other law.'" Id. (footnotes omitted). Citing Camacho v. Autor. de Tel. de Puerto Rico, 868 F.2d 482, 487-88 (1st Cir. 1989), Verizon asserts that "[t]o the extent that state laws do not contain similar exceptions or authorizations, they are preempted." Id. Verizon opines that an investigation into the matters raised by complainants would require the Commission to interpret and enforce federal statutes governing national security matters, and that the Commission lacks such authority. Id. at 8.

In concluding its argument in support of its preliminary objections, Verizon states as follows:

In sum, there is no basis to assume that Verizon has violated the law. Further, Verizon is precluded by federal law from providing information about its cooperation, if any, with this national security matter. Verizon accordingly cannot confirm or deny cooperation in such a program or the receipt of any government authorizations or certifications, let alone provide the other information [complainants] suggest that the Commission request. As a result, there would be no evidence for the Commission to consider in any investigation. Moreover, neither the federal nor state wiretapping and surveillance statutes authorizes or contemplates investigations or enforcement proceedings by the Commission to determine the lawfulness of any national security

program or of any party's alleged participation in it. Nor does the Commission possess the practical tools and ability to construe and enforce state and/or federal criminal statutes, consistent with all constitutional rights and protections. Accordingly, even if the Commission could inquire into the facts – and as discussed above it cannot – the Commission lacks the authority or jurisdiction to investigate or resolve [complainants'] allegations. Instead, ongoing Congressional oversight through the Senate and House Intelligence committees, as well as the pending proceedings in federal court that will consider the state secrets issues, are more appropriate forums for addressing any issues related to this national security program.

Id. at 8-9.

In its response to the preliminary objections of AT&T and Verizon, ACLU asserts that the Commission does have jurisdiction to hear its complaint. ACLU Response at 6. Citing 66 Pa. C.S. §3019(d) and 52 Pa. Code §63.135(2), ACLU argues that Pennsylvania law expressly protects the privacy of customer information. Id. Section 3019(d) of the Public Utility Code, 66 Pa.C.S. §3019(d), provides:

§3019. Additional powers and duties

* * *

(d) Privacy of customer information.-

(1) Except as otherwise provided in this subsection, a telecommunications carrier may not disclose to any person information relating to any customer's patterns of use, equipment and network information and any accumulated records about customers with the exception of name, address and telephone number.

(2) A telecommunications carrier may disclose such information:

(i) Pursuant to a court order or where otherwise required by Federal or State law.

(ii) To the carrier's affiliates, agents, contractors or vendors and other telecommunications carriers or interexchange telecommunications carriers as permitted by Federal or State law.

(iii) Where the information consists of aggregate data which does not identify individual customers.

66 Pa.C.S. §3019(d) (emphasis supplied).

And Section 63.135(2) of Title 52 of the Pennsylvania Code, 52 Pa. Code §63.135(2), provides:

§ 63.135. Customer information.

This section describes procedures for determining employee access to customer information and the purposes for which this information may be used by employees responding to requests for customer information from persons outside the telephone company and the recording of use and disclosure of customer information.

* * *

(2) Requests from the public. Customer information that is not subject to public availability may not be disclosed to persons outside the telephone company or to subsidiaries or affiliates of the telephone company, except in limited instances which are a necessary incident to:

(i) The provision of service.

(ii) The protection of the legal rights or property of the telephone company where the action is taken in the normal course of an employe's activities.

(iii) The protection of the telephone company, an interconnecting carrier, a customer or user of service from fraudulent, unlawful or abusive use of service.

(iv) A disclosure that is required by a valid subpoena, search warrant, court order or other lawful process.

(v) A disclosure that is requested or consented to by the customer or the customer's attorney, agent, employe or other authorized representative.

(vi) A disclosure request that is required or permitted by law, including the regulations, decisions or orders of a regulatory agency.

(vii) A disclosure to governmental entities if the customer has consented to the disclosure, the disclosure is required by a subpoena, warrant or court order or disclosure is made as part of telephone company service.

52 Pa. Code §63.135(2) (emphasis supplied).

ACLU clarifies that it seeks an investigation into: (1) whether respondents received a request for information; and (2) whether responding to the request would run afoul of Pennsylvania law, as enforced by the Commission. Id. at 6-7. ACLU opines that after the Commission resolves those two issues, it can then decide whether ACLU's request for relief is appropriate. Id. (In its request for relief included in its complaint, ACLU asks the Commission to order respondents to: (1) provide ACLU and the Commission with a complete accounting of any and all releases of customer information to the NSA or any other federal or state law enforcement agency that was not compelled by court order or warrant; (2) cease and desist from releasing customer calling information to the NSA or other law enforcement agencies without court order or warrant; and (3) take such steps as are necessary to comply with Pennsylvania law.)

ACLU further explains that:

Complainants do not ask the Commission to determine whether the NSA is entitled to make the reported demands for consumer telephone records – indeed, Complainant ACLU has pursued those claims against the NSA in a separate federal court action.

Complainants' primary request in this forum is an "accounting of any and all releases of customer information to the NSA or any other federal or state law enforcement agency that was not compelled by court order or warrant."

Id. at 12.

ACLU argues that by disclosing whether or not they disclosed customer information to the NSA or another U.S. government agency, respondents would not be divulging classified information. Id. at 7. ACLU notes that Qwest Communications Corporation and BellSouth Corporation have divulged that they did not disclose customer information to the NSA, and they have not been prosecuted for the disclosure. Id. ACLU asserts that because the U.S. President has publicly defended the legality of the NSA program, respondents would not be divulging classified information if they disclose whether or not they are participating in the program. Id. at 7-8.

ACLU also argues that respondents refer to inapplicable law in support of their preliminary objections. ACLU notes for example that the Totten rule does not apply in this case because ACLU is not seeking to enforce or interpret terms of an espionage agreement. Id. at 8. ACLU also asserts that the state secrets privilege does not apply in this case because this privilege can only be asserted by a U.S. government department head, and no U.S. government department head has intervened in this case and asserted such a privilege. Id. at 9-10.

In conclusion, ACLU argues that "[t]he complaint before the Commission focuses on the Respondents' conduct, not the NSA's, and is therefore entirely within the jurisdiction of the Commission." Id. at 13-14.

The power of the Commission is statutory; the legislative grant of power to act in any particular case must be clear. City of Philadelphia v. Philadelphia Electric Company, 473 A.2d 997, 1000 (Pa. 1984). The authority of the Commission must arise either from express words of pertinent statutes or by strong and necessary implication therefrom. Id. at 999. The Commission's statutory authority to regulate the rates and service of public utilities that provide service in Pennsylvania is found in the Public Utility Code, 66 Pa.C.S. §§101 - 3316. The Public

Utility Code does not confer upon the Commission an exclusive jurisdiction to decide all matters involving regulated public utilities. Virgilli v. Southwestern Pennsylvania Water Authority, 427 A.2d 1251,1253, 58 Pa. Commw. 340 (1981). For example, as AT&T indicated in its preliminary objections, the Commission does not have jurisdiction over matters involving allegations of illegal wiretapping. McClellan v. PUC, 634 A.2d 686, 688, 159 Pa. Commw. 675 (1993). The Wiretapping and Electronics Surveillance Control Act, 18 Pa.C.S. §§ 5701-5781, gives the courts exclusive power to determine the legality of electronic surveillance. Id.

In the present case, ACLU alleges that AT&T, Verizon and the other telecommunications carriers named in its complaint, may have violated Pennsylvania public utility law (specifically, 66 Pa. C.S. §3019(d)⁶ and 52 Pa. Code §63.135(2)) if they gave the NSA information regarding the calling patterns of Pennsylvania customers without requiring a search warrant or court order before disclosing the information. ACLU asks that the Commission open an investigation into the matter. In such an investigation, ACLU asks that the Commission first compel respondents to admit or deny that they disclosed to the NSA information regarding the calling patterns of Pennsylvania customers, without requiring a search warrant or court order. If respondents answer “yes,” ACLU asks that the Commission then determine whether respondents’ actions violated Pennsylvania public utility law. If the Commission determines that it does, ACLU asks that the Commission then grant its requested relief. The relief requested by ACLU is that respondents be ordered to: (1) provide ACLU and the Commission with a complete accounting of the customer information it provided to the NSA; and (2) cease and desist from providing the information unless a court order or search warrant is produced. ACLU emphasizes that it wants to focus on the conduct of the telecommunications carriers in this proceeding before the Commission, while focusing on the conduct of the NSA in its proceeding before the federal court.

However, in this matter in which the overarching issue of national security has been raised, the conduct of the telecommunications carriers and the conduct of the NSA are inextricably intertwined. Although the complaints are narrowly drawn to test Pennsylvania regulatory authority, the questions involved in this matter are in fact larger in scope than just

⁶ ACLU did not refer to this Statute in its complaint, but it did refer to it in its response to the preliminary objections.

whether the telecommunications carriers, who are the subject of the present complaints, violated the Public Utility Code and Commission regulations. Matters of national security are implicated in this proceeding. There is no indication in the Public Utility Code or the Commission's regulations governing the protection of customer information, that the Pennsylvania Legislature intended that the Commission would decide matters of national security. Nor is there any federal law bestowing such authority upon the Commission. The Commission clearly does not have the experience, expertise and competence to adjudicate cases involving questions of national security. The federal courts however, clearly do have the experience, expertise and competence to handle cases with national security implications.

AT&T and Verizon aver that they are prohibited by federal law governing national security matters from even admitting or denying whether they are providing customer information to the NSA. AT&T and Verizon claim that the U.S. Department of Justice has warned them that their disclosure of whether or not they are participating in any NSA-led surveillance program would be violative of federal law governing national security matters. So as a threshold matter, a determination would have to be made in this case as to whether the Commission has the authority to determine whether or not respondents refusal to comment on whether they are providing customer calling information to the NSA is a matter of national security. And as ACLU indicates, the Commission would first have to determine that the disclosure would not be a matter of national security before it could compel respondents to disclose whether or not they have provided or are providing the NSA with customer calling information. As AT&T and Verizon have noted, the President of the United States, the Director of National Intelligence and the Director of the NSA all say that this is a matter of national security. ACLU says that it is not a matter of national security. ACLU indicates that its interpretation of federal law is that because the United States President has defended the legality of the NSA program, and because other telecommunications carriers have disclosed their non-involvement in the NSA program and have not been prosecuted, AT&T and Verizon would not violate national security restrictions by disclosing whether or not they are involved in the NSA program. However, I agree with Verizon that the Commission does not have the authority to construe and interpret federal law governing national security matters. I therefore find that the Commission does not have the authority to determine whether or not respondents' refusal to

comment on whether they are providing customer calling information to the NSA is a matter of national security.

The Commission could not in this case decide the question of whether Pennsylvania public utility law was violated, in a vacuum. It would first be required to compel respondents to divulge whether or not they are providing customer calling information to the NSA. For the reasons provided herein, I find that the Commission does not have the authority to compel respondents to disclose that information over their claims of national security prohibitions.

While complainants allege in this proceeding that respondents possibly violated Pennsylvania public utility law if they provided customer calling information to the NSA without a warrant or court order, the overarching issue is whether any cooperation between the NSA and respondents involving customer calling information was legal consistent with federal law concerning matters of alleged national security. A federal court may provide ACLU with the investigation, determinations and relief that it has requested in its complaint before the Commission. If a federal court decides that the matter of respondents' cooperation or non-cooperation with the NSA in providing customer calling information is a matter of national security, then the inquiry may end there. However, if a federal court decides that it is not a matter of national security or that information may be provided under adequate protections and precautions, then a federal court may: (1) compel respondents to disclose whether or not they are giving the NSA customer calling information without requiring a search warrant or court order; (2) order respondents to provide to ACLU a complete accounting of any customer information respondents provided to the NSA without requiring a search warrant or court order; and (3) order respondents to cease and desist from providing any customer information to the NSA without requiring a search warrant or court order, if the federal court determines that the law requires such a process to be followed. The only aspect of ACLU's complaint that a federal court may or may not address is whether respondents violated Pennsylvania public utility law if they provided customer information to the NSA without requiring a search warrant or court order. However, again, the overarching question is whether federal law was violated if respondents provided customer calling information to the NSA without requiring a search warrant or court order. A federal court, and not the Commission, has jurisdiction to adjudicate that issue. (A case in which

the plaintiffs allege that AT&T is collaborating with the NSA in a massive warrantless surveillance program that illegally tracks the domestic and foreign communication records of millions of Americans, is proceeding in federal court after the federal court denied the motions of the U.S. government and AT&T to dismiss the lawsuit.) See, Hepting, et al. v. AT&T Corp., et al.⁷, Case No. C-06-672 VRW (N.D. Cal.) (July 20, 2006). For all of the foregoing reasons, I will grant the preliminary objections of AT&T and Verizon and dismiss the complaint of ACLU.

Assuming arguendo that the Commission has some decision-making authority in regard to this matter, it would only come after a federal court with binding authority over the Commission, decided: (1) that this is not a matter of national security; (2) that respondents may be compelled to disclose the nature and extent of any customer information they have provided or are providing to the NSA; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer information was provided without a search warrant or court order. If that should occur, then complainants may, if they so choose, file a new complaint based on such a federal court decision.

As earlier noted, ACLU's complaint was also filed against CTSI and InfoHighway. In its answer to the complaint, CTSI avers that it has never been contacted by the NSA and that it has not provided customer calling information to the NSA. InfoHighway's Chairman, Mr. Ginsberg, filed a letter in lieu of an answer to the complaint. In his letter Mr. Ginsberg similarly avers that InfoHighway has: (1) never been contacted by the NSA and asked to provide customer calling information or private calling records for any customer; (2) never provided any information to any governmental agency with respect to any of the account numbers listed in Exhibit B of the complaint; and (3) never provided any information to any governmental authority without being compelled to do so by a valid subpoena or court order. When ACLU received similar answers to its complaint from Denver & Ephrata Telephone & Telegraph Company and Buffalo Valley Telephone Company, albeit those answers were also accompanied by preliminary objections, ACLU withdrew its complaint as to those

⁷ In another federal court case involving similar allegations as in Hepting, but focused on AT&T's Illinois customers, the federal court held that due to the operation of the "states secrets privilege," the plaintiffs could not obtain through discovery the information they needed (regarding any submissions by AT&T of customer calling records to the U.S. government) to prove their standing to sue for prospective relief. The court consequently dismissed the complaint. See, Terkel et al. v. AT&T Corp., et al., Case No. 06 C 2837 (N.D. Ill.) (July 25, 2006).

telecommunications carriers.⁸ See, answers to complaint filed by Denver & Ephrata Telephone & Telegraph Company and Buffalo Valley Telephone Company. The record does not indicate why ACLU has not withdrawn its complaint as to CTSI and InfoHighway. However, because ACLU's complaint against CTSI and InfoHighway, like its complaint against the other remaining respondents, raises matters of national security over which the Commission has no jurisdiction, I will dismiss the complaint as to CTSI and InfoHighway.

In its complaints, CWA alleges that Verizon and AT&T possibly engaged in unreasonable utility practices if they participated in the NSA's "domestic wiretapping program." CWA asks the Commission to open an investigation, and using its "statutory authority" compel respondents to answer questions regarding the nature and extent of their cooperation with the NSA, if any. As previously stated, the Commission does not have jurisdiction over all matters involving regulated public utilities. And as also previously stated, the Commission does not have jurisdiction over matters involving allegations of illegal wiretapping. See, McClellan v. PUC, 634 A.2d 686, 688, 159 Pa. Commw. 675 (1993). Nor does the Commission have jurisdiction over matters of alleged national security, for the reasons stated above. The Commission does not have the authority to determine whether or not respondents' refusal to comment on whether they are providing customer information to the NSA is a matter of national security. Nor does the Commission have the authority to compel respondents to disclose whether or not they have provided or are providing customer information to the NSA. Consequently, the Commission does not have the authority to compel respondent to answer the four questions posed in CWA's complaints regarding the nature and extent of respondents' cooperation with the NSA, if any. Therefore, for all of the foregoing reasons, I will grant the preliminary objections of AT&T and Verizon and dismiss the complaints of CWA.

My dismissal of CWA's complaints, like my dismissal of ACLU's complaints, is without prejudice to the right of CWA to file new complaints if it obtains a federal court decision, that is binding on the Commission, which holds: (1) that this is not a matter of national security; (2) that respondent telecommunications carriers may be compelled to disclose the nature and extent of any customer calling information they have provided to and/or are providing

⁸ The record does not reflect why ACLU withdrew its complaint against United Telephone Company of Pennsylvania d/b/a Embarq Pennsylvania, which did not file an answer to the complaint.

to the NSA; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer calling information was provided without a search warrant or court order.

ORDER

THEREFORE,

IT IS ORDERED:

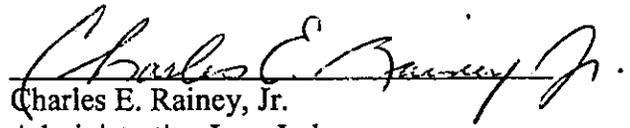
1. That the preliminary objections of AT&T Communications of Pennsylvania LLC are granted.
2. That the preliminary objections of Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc. are granted.
3. That the motion of Verizon Pennsylvania Inc., Verizon North Inc. and Verizon Select Services Inc. for the admission *pro hac vice* of Leigh A. Hyer, Esquire is granted.
4. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against AT&T Communications of Pennsylvania LLC at docket no. C-20066397 is dismissed.
5. That the complaints of American Civil Liberties Union of Pennsylvania, et al. against Verizon Pennsylvania Inc. at docket no. C-20066398, and Verizon North Inc. at docket no. C-20066399 are dismissed.
6. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against CTSI, LLC at docket no. C-20066401 is dismissed.
7. That the complaint of American Civil Liberties Union of Pennsylvania, et al. against ARC Networks Inc. d/b/a InfoHighway Communications at docket no. C-20066404 is dismissed.

8. That the complaints of District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, against Verizon Pennsylvania Inc. at docket no. C-20066410, Verizon North Inc. at docket no. C-20066411 and Verizon Select Services Inc. at docket no. C-20066412, are dismissed.

9. That the complaint of District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, against AT&T Communications of Pennsylvania LLC at docket no. C-20066413 is dismissed.

10. That the complaints of American Civil Liberties Union of Pennsylvania, et al. and District 13 of the Communications Workers of America and its Assistant to the Vice President, Terrance T. Tipping, are dismissed without prejudice to their right to file new complaints if they should obtain a federal court decision, that is binding on the Commission, which holds: (1) that this is not a matter of national security; (2) that respondent telecommunications carriers may be compelled to disclose the nature and extent of any customer calling information they have provided to and/or are providing to the National Security Agency or other government law enforcement agency; and (3) that the Commission may decide whether Pennsylvania public utility law was violated if any customer calling information was provided without a search warrant or court order.

11. That these cases be marked closed.


Charles E. Rainey, Jr.
Administrative Law Judge

Date: August 16, 2006

AP NewsBreak: SF reviews contracts with AT&T over domestic spying

- By SCOTT LINDLAW, Associated Press Writer
Tuesday, July 11, 2006



(07-11) 14:02 PDT San Francisco (AP) --

City officials are investigating AT&T's alleged cooperation with the National Security Agency and considering possible "consequences" the company could face in its extensive municipal contracts here if it is violating civil liberties, Mayor Gavin Newsom said Tuesday.

"If what I'm reading is true, I've got some serious problems as a San Franciscan, as a taxpayer and as mayor," Newsom said in interview with The Associated Press. "And I don't like it."

A federal lawsuit filed by Internet privacy advocate Electronic Frontier Foundation accuses the telecommunications giant of illegally cooperating with the NSA to make communications on AT&T networks available to the spy agency without warrants. According to the lawsuit, AT&T allowed the NSA to install data mining equipment in secret rooms at AT&T offices in San Francisco and a handful of other cities.

Last month, the government urged a federal judge to dismiss the suit, saying it threatens to reveal state secrets. The judge's decision is pending.

Newsom said he has asked City Attorney Dennis Herrera to conduct "fact-finding" on the matter. But the mayor also said he has completed his own compilation of "all of our current business relationships the city has with AT&T."

That review, which includes expiration dates and other obligations, "may be suggestive that if we conclude that this is sincerely problematic, there may be a desire to not just make a symbolic statement of opposition, but to make a substantive one."

The mayor said he did not know the value of AT&T's contracts with San Francisco. Nor would he provide a timetable for completion of the city attorney's probe.

"I recognize the ability, (from) a local perspective, to perhaps have a little more influence because we do have a strong relationship with AT&T and I'd like to continue that," he said.

"But I also think it's a two-way street," Newsom said. "If you're going do business with us, and San Francisco always has, we say, please help represent the values of the people that are actually purchasing those goods and services, meaning the taxpayers of this city."

The city attorney probably has the power to subpoena, Newsom said, adding that he did not know for sure. If true, that would mean the city might have the power to learn details of the program that have not been publicly disclosed.

The city attorney has not spoken directly to the NSA about its program, he said.

An AT&T spokesman, Michael Coe, declined to comment on the city review or the mayor's remarks.

He repeated a statement the company has issued repeatedly since published reports

linked AT&T to the government's warrantless wiretapping programs several months ago.

"The fact is, AT&T does not give customer information to law enforcement authorities or government agencies without legal authorization," the statement says. "We have a statutory requirement to assist law enforcement and other government agencies responsible for protecting the public welfare, whether it be an individual or the security interests of the entire nation."

URL:

<http://sfgate.com/cgi-bin/article.cgi?file=/news/archive/2006/07/11/financial/f140225D55.D>

©2007 Associated Press

EXHIBIT 12



Text Size: A A A A

• Cars • Computers • Gadgets • Internet • Med-Tech • Security • Space • Software • Wireless

AT&T Sued Over NSA Eavesdropping

Â

See Also

- NSA's Lamest Spy Tool: Cookies
- Secrecy Power Sinks Patent Case
- Lawbreaker in Chief
- EPIC Sues NSA Over Snooping
- Report: Bush OK'd Spying in US
- 2001: Bush Warned of Tech Dangers

By Ryan Singel Also by this reporter
16:03 PM Jan, 31, 2006

The Electronic Frontier Foundation filed a class-action lawsuit against AT&T on Tuesday, accusing the telecom company of violating federal laws by collaborating with the government's secret, warrantless wiretapping of American citizens' phone and internet usage.

The suit (.pdf), filed by the civil liberties group in federal court in San Francisco, alleges AT&T secretly gave the National Security Agency access to two massive databases that included both the contents of its subscribers' communications and detailed transaction records, such as numbers dialed and internet addresses visited.

"Our goal is to go after the people who are making the

government's illegal surveillance possible," says EFF attorney Kevin Bankston. "They could not do what they are doing without the help of companies like AT&T. We want to make it clear to AT&T that it is not in their legal or economic interests to violate the law whenever the president asks them to."

One of AT&T's databases, known as "Hawkeye," contains 312 terabytes of data detailing nearly every telephone communication on AT&T's domestic network since 2001, according to the complaint. The suit also alleges that AT&T allowed the NSA to use the company's powerful Daytona database-management software to quickly search this and other communication databases.

That action violates the First and Fourth amendments to the Constitution, federal wiretapping statutes, telecommunications laws and the Electronic Communications Privacy Act, according to the complaint.

The suit, which relies on reporting from the *Los Angeles Times*, seeks up to \$22,000 in damages for each AT&T customer, plus punitive fines.

AT&T did not immediately respond to a request for comment.

The lawsuit comes a little more than a month after *The New York Times* reported that in 2001, President Bush ordered the NSA to begin warrantless monitoring of Americans' overseas phone calls and internet usage.

The administration defends the eavesdropping program, saying it is only targeting communications to and from suspected terrorists, that government lawyers review the program every 45 days and that Congress authorized the president to track down 9/11 co-conspirators, thereby giving the president the ability to bypass wiretapping laws.

Some Senate Democrats and Republicans, along with civil libertarians and former government officials, counter that the wiretaps are simply illegal and that wiretapping warrants can be

acquired easily if the government has probable cause to believe an American is affiliated with terrorists.

The government is not named in the lawsuit, though it is already being sued by the American Civil Liberties Union over the surveillance program.

Bankston estimates that millions of people nationwide would be eligible to join the class action, pushing the possible total fines into the billions. However, he expects the administration will try to kill the lawsuit by invoking the rarely used state secrets privilege.

"If state secrecy can prevent us from preserving the rights of millions upon millions of people, then there is a profound problem with the law," says Bankston.

Â

Wired News: Contact Us | Advertising
| Subscribe | Reprints |
Customer Service | Member Services
We are translated daily into Korean and
Japanese
Wired.com Â© 2006 CondÃ©Net Inc. All
rights reserved.
Your use of this website constitutes
acceptance of our **User Agreement**
and **Privacy Policy**

MSN Tracking Image

MSNBC.com

Newsweek.com

Newsweek Poll: Americans Wary of NSA Surveillance

Bush's approval ratings hit new lows as controversy rages.

NEWSWEEK WEB EXCLUSIVE

By David Jefferson

Updated: 10:11 a.m. PT May 14, 2006

May 13, 2006 - Has the Bush administration gone too far in expanding the powers of the President to fight terrorism? Yes, say a majority of Americans, following this week's revelation that the National Security Agency has been secretly collecting the phone records of U.S. citizens since the September 11 terrorist attacks. According to the latest NEWSWEEK poll, 53 percent of Americans think the NSA's surveillance program "goes too far in invading people's privacy," while 41 percent see it as a necessary tool to combat terrorism.

President Bush tried to reassure the public this week that its privacy is "fiercely protected," and that "we're not mining or trolling through the personal lives of innocent Americans." Nonetheless, Americans think the White House has overstepped its bounds: 57 percent said that in light of the NSA data-mining news and other executive actions, the Bush-Cheney Administration has "gone too far in expanding presidential power." That compares to 38 percent who think the Administration's actions are appropriate.

There's more bad news for the White House in the NEWSWEEK poll: President Bush's approval rating has dropped to the lowest in his presidency. At 35 percent, his rating is one point below the 36 percent he received in NEWSWEEK's polls in March and November, 2005.

Iraq continues to be the biggest drain on the president's popularity: 86 percent of Americans say the Iraq situation, coupled with new information about the decision to go to war, have negatively influenced their view of the president. Asked about Bush's performance on a variety of issues, from the economy to taxes, respondents gave the president some of the worst marks of his tenure, and in no instance did approval reach more than 50 percent.

Anger over the recent spike in prices at the pump has cost the president dearly: only 17 percent of Americans approve of the way Bush is handling gas prices. Nor do they like the way he is dealing with the federal budget deficit (only 19 percent approve) or immigration policy (25 percent). Even as Congress was approving the latest Bush tax cuts this week, public opinion of his handling of taxes dropped to a record low for him of 39 percent. Half of Americans (50 percent) now think George W. Bush will go down in history as a "below-average" president.

News of the NSA's secret phone-records program comes at an especially awkward time for the president. His nominee for the top job at the CIA—former NSA head Gen. Michael Hayden—heads into confirmation hearings on the Hill next week. With Democrats expressing outrage over the surveillance program, and several Republicans voicing concern as well, the hearings could turn into something of a Congressional probe into the NSA's collection of phone data.

According to the NEWSWEEK poll, 73 percent of Democrats and 26 percent of Republicans think the NSA's program is overly intrusive. Details of the surveillance efforts were first reported on Wednesday by USA Today. The newspaper said the NSA has collected tens of millions of customer phone records from AT&T Inc., Verizon Communications Inc. and Bell-South Corp., in an effort to assemble a database of every call made within the United States. While the records include detailed information about when and where phone calls were made, the government isn't listening in to the actual conversations, a U.S.

intelligence official familiar with the program told the newspaper. The only big telecommunications company that has refused to participate is Denver-based Qwest, which says it was concerned about the legal implications of turning over customer information to the government without warrants.

The fracas over surveillance is yet another headache the Republicans didn't need heading into the November midterm elections. Seventy-one percent of Americans are dissatisfied with the way things are going in the country, and more than half—52 percent—say they would like the Democrats to win enough seats to take over Congress this November (only 35 percent want the Republicans to keep control). Looking ahead to the presidential race in 2008, more Americans said they would like to see a Democrat elected than a Republican—50 percent versus 31 percent. That, despite the fact that a majority of those polled don't believe a Democrat would do any better than Bush is doing on a variety of issues. Democrats also have a significant lead in being perceived as better able to bring about the changes the country needs: 53 percent to 30 percent.

Bush's new approval low of 35 percent in the NEWSWEEK poll is below the nadir of Bill Clinton's presidency in May 1993, when the former president hit 36 percent. The 41st president, George H.W. Bush, hit his lowest ratings late in 1992 before he was defeated by Clinton: A Gallup poll in July 1992 recorded a 32 percent approval rate for the first President Bush. But other presidents have fared worse. Jimmy Carter scored 28-29 percent in June and July 1979, according to Gallup. President Richard Nixon's Gallup number dropped to 24 percent in August 1974.

For the NEWSWEEK poll, Princeton Survey Research Associates International interviewed 1,007 adults aged 18 and older between May 11 and 12 by telephone. The margin of error is plus or minus 4 percentage points.

URL: <http://www.msnbc.msn.com/id/12771821/site/newsweek/page/2/>
© 2007 MSNBC.com

EXHIBIT 14



BOSTON COMMON

ASSET MANAGEMENT, LLC

[Home](#) > [News](#)

Human Rights and Internet Fragmentation Proposal Receives Record Shareholder Support

BOSTON, MA November 15, 2006 -- The human rights and Internet fragmentation resolution led by Boston Common Asset Management received a record level of support from shareholders, according to the preliminary vote announced at the Cisco Systems Annual Stockholders Meeting today in Santa Clara, California. Twenty-nine percent of all shareholders voted against management's recommendation and supported Boston Common's proposal with a "For" or "Abstain" vote, according to an announcement made at the meeting. "This is a record vote for a resolution of this nature" said Dawn Wolfe, Social Research Analyst at Boston Common Asset Management. "The fact that well over one-quarter of all Cisco shareholders disagree with the company's assertion that Internet fragmentation and human rights liabilities do not represent a potential threat to Cisco's long term global growth is a strong statement," Wolfe continued.

The proposal, co-filed by four additional investors, asks management to disclose the concrete steps it could reasonably take to reduce fragmentation of the Internet, the suppression of information, or violations of personal privacy. Internet fragmentation, or balkanization, occurs when government authorities create extensive firewalls around citizens, severely restrict the flow of information, conduct pervasive surveillance of electronic communication users, and ultimately slow the growth of people accessing the Internet. Boston Common began formal engagement with Cisco in January 2005 over the human rights and long term financial impacts of selling powerful networking technology to repressive governments.

For more information please contact Dawn Wolfe, Boston Common Asset Management, (617) 720-5557, [dwolfe\(at\)bostoncommonasset.com](mailto:dwolfe(at)bostoncommonasset.com)

[Home](#) | [About Us](#) | [Investment Services](#) | [Social Screening & Advocacy](#) | [News](#) | [Newsletter](#) | [Active Investor Social Update](#) | [Contact Us](#)

Copyright © 2006 **Boston Common Asset Management, LLC**
84 State Street, Suite 1000, Boston, MA 02109
Tel: 617-720-5557 Fax: 617-720-5665



RECEIVED
2007 JAN 23 PM 3:09
COUNSEL
S. W. BIRNBAUM

Wayne A. Wirtz
Assistant General Counsel
Legal Department
175 E. Houston, Room 205
San Antonio, Texas 78205
(210) 351-3736
(210) 351-3467

1934 Act/ Rule 14a-8

January 19, 2007

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, DC 20549

Re: AT&T Inc. 2007 Annual Meeting – Stockholder Proposal of Jeremy Kagan
on Behalf of As You Sow Foundation

Ladies and Gentlemen:

We refer to the recent letter, dated January 9, 2007, from Jonas D. Kron, on behalf of As You Sow Foundation, Jeremy Kagan, Jeffery Hersh, Calvert Asset Management Company, Inc., Larry Fahn, The Adrian Dominican Sisters and Camilla Madden Charitable Trust (the "Proponents") asking the Staff not to concur in AT&T Inc.'s ("AT&T") conclusion, as described in our letter to you of December 11, 2006, that AT&T may omit the proposal submitted by As You Sow, on behalf of Jeremy Kagan, on October 27, 2006 (the "Proposal") from the proxy statement for its 2007 Annual Meeting.

Pursuant to Rule 14a-8(j), enclosed are six copies of this letter. A copy of this letter is also being mailed concurrently to Jonas D. Kron.

This letter addresses the issues raised by Mr. Kron in his January 9, 2007 letter and should be read in conjunction with AT&T's original letter dated December 11, 2006.

Mr. Kron's extensive letter objects to AT&T's exclusion of the Proposal on each of the grounds asserted by AT&T. We believe Mr. Kron's points do not warrant a similarly extensive response, as we have already set forth our position on them in our December 11th letter. Nevertheless, we set forth below our general views regarding Mr. Kron's letter.

The Proposal May be Omitted Pursuant to Rule 14a-8(i)(2) Because Implementing the Proposal Would Cause AT&T to Violate Federal Law.

Mr. Kron's argument against exclusion of the Proposal under Rule 14a-8(i)(2) lacks merit because it fails to address most of the arguments made and the relevant legal authority cited in the legal opinion of Sidley Austin LLP, which was attached as Attachment A to AT&T's letter dated December 11, 2006 (the "Sidley Austin Opinion"). Rather than address the arguments made in the Sidley Austin Opinion, Mr. Kron's letter attacks strawman positions upon which the Sidley Austin Opinion does not rely, misconstrues a federal court decision that does not address the relevant issues, and attempts to recast the Proposal in a manner that is inconsistent with its plain language and import. Mr. Kron's arguments do nothing to contradict AT&T's original position that implementing the Proposal would cause AT&T to violate the law. Having considered the arguments made in Mr. Kron's letter, Sidley Austin has nevertheless confirmed their earlier opinion that implementing the Proposal would cause AT&T to violate numerous federal laws (a copy of the confirming Sidley Austin opinion is enclosed with this letter as Exhibit 1).

The Proposal May be Omitted Pursuant to Rule 14a-8(i)(7) Because it Relates to Ordinary Business Matters.

The Proposal relates to ordinary business matters of customer privacy and does not implicate any significant public policy concerns.

Mr. Kron's arguments with respect to the Proposal's "substantial policy considerations" seem to mischaracterize the magnitude of the privacy concerns purported to be implicated by the Proposal. On the contrary, these concerns do not rise to the level of significance required to overcome a company's ability to exclude a proposal as relating to matters of its ordinary business. The Staff has already concluded in Bank of America Corp. (February 21, 2006) that any social policy concerns implicated by a shareholder proposal very similar to the Proposal were not significant enough to override management's legitimate need for overseeing the company's daily business operations. Responding to several recent security breaches involving the company, the proposal in Bank of America Corp. requested the company to report on its "policies and procedures for ensuring that all personal and private information pertaining to all Bank of America customers will remain confidential." Similarly, the Proposal requests AT&T to produce a report assessing customer privacy issues and AT&T's policies and procedures for addressing such issues in response to a perceived breach of that privacy. The policy considerations purportedly implicated by the Proposal are no more "substantial" than those which the Staff considered in making its determination that Bank of America could nevertheless exclude the proposal under Rule 14a-8(i)(7).

The fact that the Proposal also asks for a description of "additional policies," as Mr. Kron highlights, does not distinguish the Proposal from the one excluded in

Bank of America Corp. in any meaningful way. Consideration of any policies and/or procedures regarding the privacy of customer records is a fundamental part of a company's day-to-day business operations, regardless of whether the company is reciting its current policies or evaluating the possibility of additional policies.

Furthermore, although Mr. Kron's letter cites Cisco Systems Inc. as support for his position, it conveniently ignores the numerous precedents cited by AT&T where the Staff has allowed companies to omit shareholder proposals that address ordinary business matters, even though they might also implicate public policy concerns: Microsoft (September 29, 2006) (excluding a proposal asking the company to evaluate the impact of expanded government regulation of the internet); Pfizer Inc. (January 24, 2006) and Marathon Oil (January 23, 2006) (excluding proposals requesting inward-looking reports on the economic effects of HIV/AIDS, tuberculosis and malaria pandemics on the companies' business strategies and risk profiles).

The Proposal relates to ongoing litigation involving AT&T.

Mr. Kron's objection to AT&T's argument that the Proposal relates to the company's ongoing litigation is that the "Proposal does not expressly, let alone impliedly, request the Company to...do anything that could be said to involve whether or how the Company will litigate the cases." However, contrary to Mr. Kron's opinion, the Proposal does request AT&T to do just that – specifically, it requires AT&T to produce a report on the very same matters which are the very heart of the multiple pending lawsuits and other proceedings that AT&T is currently defending. Compliance with the Proposal would require AT&T to produce information that goes directly to the substance of these lawsuits and other proceedings, thereby dictating how the company will proceed with the discovery process in these various litigations. In fact, Mr. Kron concedes that AT&T has supplied numerous examples of cases in which the Staff has permitted the exclusion of shareholder "proposals requesting certain actions to be taken by the company that were expressly and directly linked to specific actions in specific pending or contemplated litigation." Rather than addressing AT&T's argument that the Proposal interferes with the company's ongoing litigation by essentially sidestepping the discovery process, Mr. Kron simply concludes that the Proposal does not require AT&T to do anything that would affect its current litigation strategy.

Moreover, in his lengthy discussion and rebuttal of the cases cited by AT&T, Mr. Kron fails to point out that the standard announced in all of those cases is that a company may exclude a shareholder proposal under the ordinary business exception of Rule 14a-8(i)(7) when the subject matter of the proposal is the same as or similar to that which is at the heart of litigation in which the company is then involved. The Proposal satisfies this standard. Although Mr. Kron attempts to re-characterize the Proposal in more innocuous terms (the Proposal contemplates "reporting on the overarching policy issues, descriptions of alternative future

policies, and general descriptions of past expenditures”), the full text of the Proposal makes it abundantly clear that the Proposal addresses exactly the same subject matter and seeks exactly the same information that is central to the multiple pending lawsuits and other proceedings in which AT&T is currently involved.

The Proposal relates to matters of legal compliance.

Mr. Kron makes the assertion that the Proposal can not be excluded as relating to the ordinary matters of conducting a legal compliance program because, as distinguished from the proposals in the numerous no-action precedents cited by AT&T, the Proposal requests a report on additional measures that the company can take to ensure customer privacy within its “existing legal compliance mechanism.” However, Mr. Kron does little more than simply state his point without providing any explanation as to why discussion of a company’s existing legal compliance mechanism relates any less to matters of legal compliance than the creation of new legal compliance structure. Proposals requesting the company to report on matters of its compliance with the law and of its relationship with government agencies, whether within a legal compliance structure that the company currently has in place or one which the proposal requests the company to develop, relate to matters of ordinary business. As Mr. Kron’s letter itself points out, the Staff has permitted both the exclusion of shareholder proposals that require the company to report on its current legal compliance policies and those that require the company to establish new ones. Therefore, the distinctions that Mr. Kron draws between the cases cited by AT&T in support of its argument and the Proposal are largely irrelevant.

The Proposal involves AT&T in the political or legislative process.

Mr. Kron’s objection to excluding the Proposal as involving AT&T in the political or legislative process is that the Proposal “does not seek an evaluation, expressly or implicitly, of any legislative or regulatory proposals.” This notion is misguided. It is clear from the terms of the Proposal and the cover letter accompanying the Proposal that the Proponents believe that AT&T has participated in government surveillance programs, which the Proponent’s oppose, and they request management to evaluate the impact that these alleged programs would have on the company’s business operations and its customers. This is certainly the type of involvement in the political process that the Staff has categorized as a matter of ordinary business, which is best left to the judgment of management. See, International Business Machines Corp. (March 2, 2000); Electronic Data Systems Corp. (March 24, 2000); Niagara Mohawk Holdings, Inc. (March 5, 2001).

The Proposal May be Omitted Pursuant to Rules 14a-8(i)(3) and 14a-8(i)(6) Because it is Vague and Indefinite and, As Such, Impossible for AT&T to Implement

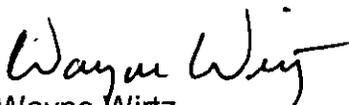
In his objection to AT&T's exclusion of the Proposal as vague and indefinite, Mr. Kron once again completely ignores AT&T's line of reasoning and focuses instead on a painstaking analysis of every minute aspect in which the Proposal differs from the proposals excluded in the precedents cited by AT&T. In fact, AT&T cited these cases simply to illustrate the Staff's long-held position that the terms of the proposal can be so vague and indefinite so as to justify its exclusion pursuant to Rule 13a-8(i)(3)'s prohibition on false and misleading statements. When read as a whole, the Proposal is intrinsically and irreconcilably contradictory. Mr. Kron has failed to point anything in the Staff's interpretations that indicates that the only basis for excluding a proposal under the vague and indefinite standard is when individual words contained in the proposal are subject to differing definitions. To the contrary, the standard adopted by the Staff is that a proposal can be excluded if "the resolution contained in the proposal is so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (CF) (September 15, 2004). The Proposal satisfies this standard.

As previously discussed above, Mr. Kron's arguments as to why the information required by the Proposal is not confidential are unconvincing. Therefore, the Proposal by its own terms, is inherently contradictory - according to the Proposal, AT&T is, at the same time, required to provide information and permitted to exclude the same information. The resolution's conflicting mandates make the Proposal inherently vague and indefinite and, as such, impossible for AT&T to implement.

* * *

For the reasons set forth above, AT&T continues to believe that it may omit the Proposal from its 2007 proxy statement under Rule 14a-8. Please acknowledge receipt of this letter by date-stamping and returning the extra enclosed copy of this letter in the enclosed self-addressed envelope.

Sincerely,


Wayne Wirtz
Assistant General Counsel

Enclosures

cc: Jonas D. Kron



SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
(202) 736 8000
(202) 736 8711 FAX

emcnicholas@sidley.com
(202) 736-8010

BEIJING	GENEVA	SAN FRANCISCO
BRUSSELS	HONG KONG	SHANGHAI
CHICAGO	LONDON	SINGAPORE
DALLAS	LOS ANGELES	TOKYO
FRANKFURT	NEW YORK	WASHINGTON, DC

FOUNDED 1866

January 22, 2007

Board of Directors
AT&T Inc.
c/o James D. Ellis
General Counsel
175 E. Houston, Room 205
San Antonio, Texas 78205

Re: Shareholder Proposal

Ladies and Gentlemen:

By our letter of November 22, 2006, we provided our legal opinion ("Legal Opinion") regarding a shareholder proposal submitted by Jeremy Kagan along with several co-filers on October 24, 2006 (the "Proposal") to AT&T, Inc. for inclusion in its 2007 proxy statement.

We have now been asked to review the conclusions in our Legal Opinion in light of the submission to the United States Securities and Exchange Commission regarding the Proposal made by Jonas D. Kron, dated January 9, 2007 ("Kron Letter"). Nothing contained in the Kron Letter causes us to change the conclusions set forth in our Legal Opinion.

This letter is subject to, and we incorporate herein by reference, all of the provisions, conditions and limitations set forth in our Legal Opinion.

Very truly yours,

A handwritten signature in cursive script that reads "Sidley Austin LLP".

Sidley Austin LLP

Jonas D. Kron, Attorney at Law

P.O. Box 42093
Portland, Oregon 97242
(971) 222-3366
jdkron@kronlaw.net

RECEIVED
2007 FEB -6 PM 3:37
U.S. SECURITIES AND EXCHANGE COMMISSION

February 5, 2007

U.S. Securities and Exchange Commission
Division of Corporation Finance
Office of Chief Counsel
100 F Street, N.E.
Washington, D.C. 20549

Re: Shareholder Proposal Submitted to AT&T Inc. for 2007 Proxy Statement

Dear Sir/Madam:

On behalf of AT&T shareholders As You Sow Foundation, Jeremy Kagan, Jeffery Hersh, Calvert Asset Management Company, Inc., Larry Fahn, The Adrian Dominican Sisters, and Camilla Madden Charitable Trust ("Proponents") this letter is a response to AT&T Incorporated's ("the Company") second letter on this matter, dated January 19, 2007, which was inexplicably not received by this office until January 31st, a full 12 days later.

Pursuant to Rule 14a-8(k), enclosed are six copies of this letter and enclosure. A copy of these materials is being mailed concurrently to AT&T Inc. Assistant General Counsel Wayne A Wirtz.

In the interest of time I have responded to the Company's January 19th letter as quickly as possible, but would like to take this opportunity to express distaste at the way in which this matter has transpired, and my concern that the Proponents have indeed been prejudiced.

On February 2, 2007 I received a phone call from Special Counsel Ted Yu asking when I received AT&T's January 19th letter. I informed him that I received the letter on January 31, 2007 and that the envelope was USPS post-marked January 25, 2007 (see attached copy of the postmarked envelope from AT&T). Mr. Yu informed me that the Staff had received the letter on January 23, 2007 – apparently two days before it was mailed to me.

Query: why is it that AT&T could not deliver its January 19th letter to me (or to the Proponents themselves) via overnight delivery as it had done with the original no-action request of December 11, 2006? Could the Company not have sent the letter, only 5 pages in length, via e-mail or fax, to allow for a timely delivery? How can the Company explain the fact that they did not even send a copy of their January 19th letter via the U.S. mail (i.e. in the slowest manner possible) until 2 days *after it was*

received by SEC Staff. The result of AT&T's conduct has been to prejudice the Proponents by hampering our ability to prepare a timely reply in a time-critical proceeding before the SEC Staff.

While the Company's strenuous attempts to bolster its original contentions and, regretfully, disparage our intentions and analysis are noted, we continue to stand by our January 9th letter to the Staff. Mindful of the need for conciseness, we would respectfully like to address the Company's latest assertions as briefly as possible.

I. The Company Can Implement the Proposal Without Violating the Law.

Contrary to the Company's contention that the Proponents did not adequately address its arguments on Rule 14a-8(i)(2), the comprehensive analysis we provided was in direct response to the very few specific arguments made by the Company. For the most part, AT&T and Mr. Austin made a lengthy presentation of some aspects of national security law without making any attempt to connect that law to the facts of this case. In those rare instances that they did, we responded fully and directly and, accordingly, will let our January 9th letter speak for itself (see especially pages 4 - 9).

Similarly, because of the brevity of AT&T's assertions it is not at all clear in what way the Company believes we misconstrued the Hon. Judge Walker's July 20, 2006 Order. If the Company believes that Judge Walker's lengthy and well reasoned opinion stands for something different, it is imperative that they share their interpretation with us at this time. All parties would appreciate at least some explanation of how the Company interprets Judge Walker's decision. The Company has had the opportunity to explain why the findings in the Order are inapplicable and has not done so. In contrast, we have provided the Staff with a full discussion of the Order and respectfully request the Staff concur with that analysis.

Additionally, the Company has failed to demonstrate how we attempted to "recast" the Proposal – it simply asserts that baseless accusation. We believe the Proposal is clear and informative and have successfully responded to AT&T's attempts to confound or confuse its meaning. To reiterate, the Proposal reads as follows:

RESOLVED: That shareholders request that the Board of Directors issue a report to shareholders in six months, at reasonable cost and excluding confidential and proprietary information, which describes the following:

- The overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies;
- Any additional policies, procedures or technologies AT&T could implement to further ensure (a) the integrity of customers' privacy rights and the confidentiality of customer information, and (b) that customer information is only released when

required by law; and

- AT&T's past expenditures on attorney's fees, experts fees, operations, lobbying and public relations/media expenses, relating to this alleged program.

There is nothing in our letter that runs contrary to this language. If the Company disagrees, it is incumbent upon AT&T to provide some specificity so that we may respond. We are unable to do anymore than disagree with such bald assertions and respectfully request the Staff to concur with our position.

In sum, it is abundantly clear that the Company would be able to implement the Proposal without violating the law. Whether it be the compelling conclusions of the Hon. Judge Walker or the plain meaning of the Proposal, in both cases it is apparent that the Proposal simply asks the Company to discuss the privacy issues facing the Company at an appropriately general level that will not violate the law. These issues are already being discussed in the public square, in Congress, in several courts and they rightfully should be discussed by the Company with its shareholders as well.

II. The Proposal is Focused on Significant Social Policy Issues.

The Company next contends that our arguments "mischaracterize the magnitude of the privacy concerns". While the Company may wish that this issue did not garner so much scrutiny, its opinion apparently is not shared by 67% of Americans, the media, members of Congress, federal regulators, state utility regulators or investors who all seem to think that it is a significant issue that warrants attention. One only needs to open the newspaper or do a brief online search to confirm that this issue continues to attract considerable attention, in the media and elsewhere, on a regular basis. We believe the lengthy examples previously provided to the Staff (see our January 9th letter at pages 11 and 12) more than demonstrate that the proposal addresses "significant policy, economic or other implications". *Roosevelt v. E.I. DuPont de Nemours & Company*, 958 F. 2d 416 (DC Cir. 1992) at 426.

With respect to the Company's reference to *Bank of America Corp.* (February 21, 2006) we stand by our analysis that it is not analogous to our Proposal because it was limited to a recitation of compliance policies. As discussed at length in our January 9th letter, such proposals are properly excluded. In addition, that proposal did not raise Constitutional issues or concerns about fundamental American rights and thus to say that the two proposals address the same subject matter is simply false. Furthermore, the dearth of any meaningful discussion of the issues raised in *Bank of America* by that proposal's proponent means that the Staff's conclusion was reached without the benefit of a complete discussion of privacy issues. Consequently, that proposal cannot be the basis for an exclusion in this matter.

We also note that the Company did not dispute our analysis regarding *Applied Digital Solutions, Inc.* (March 25, 2006) which demonstrated that the Company erroneously cited to that ruling. Nor have they objected to the applicability of *Cisco Systems Inc.* (July 13, 2002) which stands for the proposition that constitutional protections and respect for individual rights are indeed

significant social policy issues. Accordingly, we respectfully request the Staff conclude that the weight of past no-action letters is on the Proponents' side and concur that this Proposal is permissible.

Finally, the Company's references to *Microsoft* (September 29, 2006); *Pfizer Inc.* (January 24, 2006); and *Marathon Oil* (January 23, 2006) are completely misplaced because those proposals evidently did not implicate any significant social policy issues. With respect to *Microsoft*, that proposal, similar to *Bank of America Corp.* (February 21, 2006), was focused exclusively on financial issues and did not address large social policy issues like the United States Constitution and US citizens' fundamental right to privacy. Similarly, the *Pfizer* and *Marathon Oil* proposals were focused on "the *economic* effects of the HIV/AIDS, Tuberculosis and Malaria pandemics on our Company's *business* strategy." (emphasis added). Those two proposals were excluded as implicating an "evaluation of risk" - a unique circumstance that was addressed in Staff Legal Bulletin 14C. The Company has not made any evaluation of risk argument and therefore the proposals in those cases are irrelevant. Consequently, to equate these three proposals, which were focused solely on company specific financial issues as opposed to significant policy issues that transcend the ordinary business of the company, is to misapprehend the meaning of those proposals.

We would urge the Staff, especially in light of the Second Circuit's reaffirmation in *AFSCME v. AIG*, Docket No. 05-2825-cv of the importance of the Staff adhering to its 1976 and 1998 Interpretive Releases, and to base its decision here on the rule that companies may only exclude proposals that "do not involve *any* substantial policy or other considerations". 1976 Interpretive Release (emphasis added). Under that standard, the Company has simply not met its burden. It remains clear that these issues are beyond all doubt significant social policy issues that have captured the attention of millions of Americans, as well as elected representatives at the federal, state and local levels. There is no doubt whatsoever that consumer privacy is also of major concern to investors.¹

III. The Proposal Does not Wrongfully Relate to Ongoing Litigation.

With respect to the Company's reiteration of its litigation argument we do not have anything to add. The Proposal speaks for itself and contrary to the Company's assertion, we have not misrepresented or, in any way, mischaracterized its appropriate level of generality or its rightful focus on significant policy issues, as opposed to litigation details. We stand by our thorough and accurate analysis of no-action letters concerning litigation. It is evident from that analysis that the Proposal is appropriate because it does not request the Company to bring an action in court, to sue anyone, to make settlement payments, to implement regulations, forgo appellate rights or do anything that could be said to involve whether or how the Company will litigate the cases. While the

¹ A very recent demonstration of investor concern can be found in the January 17, 2007 report released by one of the largest asset management firms in Europe, F&C Asset Management plc. This report, entitled *Managing Access, Security & Privacy in the Global Digital Economy*, focuses on the core risks facing technology, media and telecom companies surrounding the issues of access, security and privacy. <<http://www.itsecurity.com/press-releases/press-release-access-privacy-telecommunications-011707/>>

Company would seem to prefer that the Rule exclude proposals that in some way implicate litigation, it simply does not do that.

IV. The Proposal Appropriately Requests that the Company Consider Additional Policies Within the Company's Existing Compliance Structure.

The Company contends that the distinctions we have made with respect to legal compliance issues are irrelevant. We respectfully disagree. It is clear from many Staff letters that the distinction we drew is a valid and meaningful one. We will not take up the Staff's time with a recitation of our analysis and would ask the Staff to review Section II.B.3 of our January 9th letter and concur with the analysis therein.

V. The Proposal is Proper Because it Does Not Seek an Evaluation of a Specific Legislative Proposal.

Despite the Company's attempt to draw attention away from the law on this issue and cast aspersions on the Proponent's intentions, the fact remains that the SEC Staff has concluded on numerous occasions that proposals which *do* involve companies in the political or legislative process are permissible. The Company does not take any steps in its letter to distinguish the cases we cite or refute our analysis and therefore our conclusions stand. As previously explained in our January 9th letter, the Proposal does not seek an evaluation, expressly or implicitly, of *any* legislative or regulatory proposal and therefore must be ruled as permissible. Under Rule 14a-8(g) "the burden is on the company to demonstrate that it is entitled to exclude a proposal" and it is clear in this line of argument, as in all of the Company's arguments, that it has not met this burden.

VI. The Proposal Does Not Violate the Law and Has Struck the Proper Balance Between Specificity and Generality, Therefore the Company Has the Power and Authority to Implement The Proposal.

The Company finally argues that we have ignored the Company's line of reasoning with respect to vagueness. We could not disagree more. In response we would simply point the Staff and the Company to the second and last paragraphs of Section III of our January 9th letter as an example of how we addressed AT&T's argument. The Company's entire vagueness argument is based upon the premise that that the "state secrets" privilege makes any discussion of these issues forbidden and therefore the Proposal has irreconcilable conflicts within its requests that would result in a meaningless report. Our primary response to the Company's vagueness argument (the "state secrets" argument) is contained in Section I of our January 9th letter and therefore we appropriately referred to Section I of our January 9th letter. The essence of our analysis is that Judge Walker concluded that the existence of the Programs and AT&T's participation is not a secret. As such, it is not impossible to implement the Proposal. Rather, the Company can implement the Proposal and respect the needs of confidentiality without misleading shareholders, violating the law or creating a meaningless report. Therefore, Rules 14a-8(i)(3) and 14a-8(i)(6) do not apply and cannot be a basis for excluding the Proposal.

Conclusion

For the reasons given above and in our more extensive letter of January 9, 2007 the Proponents, with all respect, request that the Staff inform the Company that SEC proxy rules require denial of AT&T's no-action request. As demonstrated in our two letters, the Proposal focuses on a critical social policy issue facing the nation and the Company and does so in a manner that does not cause AT&T to violate the law and does not mislead shareholders. Consequently, the Company has not met its burden under Rule 14a-8. Therefore, we are of the opinion that the Proposal must be included in the Company's 2007 proxy materials.

As previously noted, we request that this matter be taken up by the full Commission in the event that the Staff is inclined to rule in the Company's favor.

Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information. Thank you for your consideration of this matter.

Sincerely,



Jonas Kron
Attorney at Law

enclosure

cc: Wayne A. Wirtz, Assistant General Counsel, Legal Department, AT&T Inc.
As You Sow senior staff
As You Sow Board of Directors
Adrian Dominican Sisters
Calvert Group
Jeremy Kagan
Larry Fahn
Jeffrey Hersh

**DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS**

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the Company in support of its intention to exclude the proposals from the Company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes administered by the Commission, including argument as to whether or not activities proposed to be taken would be violative of the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversary procedure.

It is important to note that the staff's and Commission's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly a discretionary determination not to recommend or take Commission enforcement action, does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the management omit the proposal from the company's proxy material.

**DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS**

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the Company in support of its intention to exclude the proposals from the Company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes administered by the Commission, including argument as to whether or not activities proposed to be taken would be violative of the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversary procedure.

It is important to note that the staff's and Commission's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly a discretionary determination not to recommend or take Commission enforcement action, does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the management omit the proposal from the company's proxy material.

February 9, 2007

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: AT&T Inc.
Incoming letter dated December 11, 2006

The proposal requests that the board issue a report containing specified information regarding disclosure of customer communications to specified government agencies without a warrant, possible steps to ensure customers' privacy rights and the confidentiality of customer information, and AT&T's past expenditures (including attorney's fees and expert's fees) relating to the "alleged program" described in the proposal.

There appears to be some basis for your view that AT&T may exclude the proposal under rule 14a-8(i)(7), as relating to AT&T's ordinary business operations (i.e., litigation strategy). Accordingly, we will not recommend enforcement action to the Commission if AT&T omits the proposal from its proxy materials in reliance on rule 14a-8(i)(7). In reaching this position, we have not found it necessary to address the alternative bases for omission upon which AT&T relies.

Sincerely,



Amanda McManus
Attorney-Adviser

END