DIVISION OF
CORPORATION FINANCE

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

February 7, 2008

Paul Wilson
Senior Attorney
Legal Department
AT&T Inc.
175 E. Houston, Room 222
San Antonio, TX 78205

Re: AT&T Inc.
Incoming letter dated December 18, 2007

Dear Mr. Wilson:

This is in response to your letters dated December 18, 2007 and January 18, 2008 concerning the shareholder proposal submitted to AT&T by the Adrian Dominican Sisters, Calvert Asset Management Company, Inc., and Larry Fahn. We also have received letters on the proponents' behalf dated January 7, 2008 and January 23, 2008. 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.

Sincerely,

Jonathan A. Ingram
Deputy Chief Counsel

Enclosures

cc: Jonas Kron
Attorney at Law
2940 SE Woodward Street
Portland, OR 97202

February 7, 2008

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: AT&T Inc.
Incoming letter dated December 18, 2007

The proposal requests that the board of directors prepare a report that discusses, from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers.

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., procedures for protecting customer information). 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,

Heather L. Maples
Special Counsel

Paul Wilson
Senior Attorney
Legal Department
AT&T Inc.
175 E. Houston, Room 222
San Antonio, Texas 78205
Phone: (210) 351-3326

1934 Act/ Rule 14a-8

December 18, 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. 2008 Annual Meeting
Shareholder Proposals of Adrian Dominican Sisters and Calvert Asset Management Company, Inc.

Ladies and Gentlemen:

This statement and the material enclosed herewith are submitted on behalf of AT&T Inc. ("AT&T" or the "Company") pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended. AT&T has received a shareholder proposal (the "ADS Proposal") from the Adrian Dominican Sisters ("Proponent ADS"), purportedly as co-sponsors with As You Sow. The Company notes that while the cover letter to the ADS Proposal indicates that As You Sow is the primary proponent of this Proposal, it has not received any proposals from As You Sow for inclusion in its 2008 proxy statement nor any correspondence from As You Sow in this regard. Proponent ADS has requested that all communications be directed to Jonas D. Kron, Attorney at Law and Sister Annette M. Sinagra. Subsequently, AT&T received an identical shareholder proposal (the "Calvert Proposal," and together with the ADS Proposal, the "Proposals") from Calvert Asset Management Company, Inc. ("Proponent Calvert," and together with Proponent ADS, "Proponents"). Although the Proposals are identical, Proponent Calvert does not identify itself as a co-sponsor with As You Sow or Proponent ADS. Proponent Calvert has requested that all communications be directed to Aditi Vora.

For the reasons stated below, AT&T intends to omit the Proposals from its 2008 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 the Proposals, 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, whether or not AT&T participated in any such programs, implementation of the Proposals would cause it to violate federal statutes prohibiting the disclosure of information relating to such programs.

Pursuant to Rule 14a-8(j), enclosed are six copies of each of: this statement, the opinion of Sidley Austin LLP, Proponents' letters submitting the Proposals and related correspondence. A copy of this letter and related cover letter are being mailed concurrently to Jonas D. Kron, Sister Annette M. Sinagra and Aditi Vora advising them of AT&T's intention to omit the Proposals from its proxy materials for the 2008 Annual Meeting.

The Proposals

On November 21, 2007, AT&T received a letter from Proponent ADS containing the ADS Proposal, which requests that the Company's Board of Directors (the "Board") report on certain policy issues relating to the disclosure of customer records and communications to federal and state agencies. That same day, AT&T also received a letter from Proponent Calvert containing the Calvert Proposal, which is identical to the ADS Proposal. Because the two Proposals and their Supporting Statements are identical, the Company will address the reasons for excluding both Proposals in this letter.

In the Proposals' Supporting Statements, Proponents point to allegations that AT&T provided customer phone records and communications data to the National Security Agency (the "NSA") as the primary basis for requesting the report. Specifically, the Proposals state:

> RESOLVED: That shareholders of AT&T (the "Company") hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. The report should be prepared at reasonable cost and made available to shareholders within six months of the annual meeting, and it may exclude proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy.[1]

[1] The full text of the ADS Proposal and its Supporting Statement and the full text of the Calvert Proposal and its Supporting Statement are attached to the Sidley Austin Opinion as Exhibit 1.

In October 2006, As You Sow, on behalf of shareholder Jeremy Kagan, requested that AT&T include a substantially similar proposal in its proxy statement for the Company's 2007 Annual Meeting; Proponents were both co-sponsors of that proposal.[2] AT&T subsequently informed the Staff of its intention not to include that proposal in its 2007 proxy statement for reasons identical to those outlined in this letter, and the Staff agreed that "AT&T may exclude the proposal under [R]ule 14a-8(i)(7), as relating to AT&T's ordinary business operations (i.e., litigation strategy)." *AT&T Inc.* (February 9, 2007). Proponents have now slightly modified the proposal submitted in 2006 to allow the Board to exclude from the required report not only proprietary and confidential information, but also classified information and information revealing the Company's litigation, regulatory or lobbying strategy. However, as further discussed below, allowing for exclusion of these additional types of information from the required report only makes the Proposals more vague and indefinite so as to make it impossible for AT&T to implement them. While AT&T believes that the Proposals can be excluded on this basis alone, they may also be properly excluded for all of the other reasons stated below.

The Proposals May be Omitted from the Proxy Statement Pursuant to Rules 14a-8(b) and 14a-8(f): Proponents failed to establish continuous share ownership for one year prior to the date the Proposals were submitted.

Rule 14a-8(b)(1) provides that in order to be eligible to submit a shareholder proposal, a shareholder must have continuously held at least $2,000 in market value or 1% of the company's securities entitled to vote on the proposal for at least one year prior to the date the shareholder submits the proposal. Pursuant to Rule 14a-8(b)(2), if the shareholder is not a registered holder of company securities, the shareholder can submit a written statement from the "record" holder of the securities verifying that, at the time the proposal was submitted, the securities have been held continuously for at least the requisite time period.

Proponent ADS failed to establish that it has owned its requisite shares of Company stock continuously for one year prior to the date of submission of the ADS Proposal.

Proponent ADS submitted the ADS Proposal to the Company by letter, dated November 15, 2007, along with six letters from Comerica Bank (the "Comerica Letters") purporting to verify that Proponent ADS satisfies the eligibility requirements of Rule 14a-8(b)(1). The ADS Proposal, along with its cover letter and the Comerica Letters, was sent by fax and by mail. The documents were faxed after business hours on November 20, 2007 to a fax number that does not belong to the Company's Corporate Secretary and that was not included in the Company's 2007 proxy statement; it was received on November 21, 2007. The documents were mailed on November 21, 2007 and received by AT&T on

[2] As noted above, As You Sow, while identified as the primary proponent of the ADS Proposal in the ADS Proposal's cover letter, has not submitted any proposals to the Company for inclusion in its 2008 proxy materials.

November 26, 2007. Each of the Comerica Letters reads as follows: "[T]he above referenced account currently holds [ ] shares of AT&T, common stock. The attached list indicates the date the stock was acquired." A bank statement indicating the dates on which the account holder acquired the shares of AT&T common stock was attached to each Comerica Letter.[3]

In accordance with Rule 14a-8(f)(1), AT&T gave timely notice to Proponent ADS of the requirement to establish eligibility under Rule 14a-8(b) in a letter, dated November 21, 2007. The letter informed Proponent ADS that the regulations of the Securities and Exchange Commission (the "Commission") required Proponent ADS to provide the Company with documentary proof that it owned the requisite amount of Company stock continuously for at least one year prior to submitting its Proposal within 14 days from receipt of the Company's deficiency letter.[4]

In response to the Company's deficiency letter, on November 29, 2007, Proponent ADS submitted a new cover letter, dated November 26, 2007, attaching its original cover letter, dated November 15, 2007, the ADS Proposal and the same Comerica Letters and attached bank statements as were originally submitted.[5]

AT&T believes that Proponent ADS failed to establish its eligibility under Rule 14a-8(b) because the Comerica Letters submitted by Proponent ADS are fatally defective for two reasons.

First, while the bank statements attached to the Comerica Letters do indicate that Proponent ADS purchased the requisite amount of AT&T stock more than one year before the date Proponent ADS submitted the ADS Proposal to the Company, neither the Comerica Letters nor the bank statements attached thereto satisfy the requirements of Rule 14a-8(b) as they are not sufficient to establish that Proponent ADS *continuously* held those shares for one year prior to submitting the Proposal.

In Staff Legal Bulletin No. 14, the Staff has explicitly stated that a shareholder's monthly, quarterly or other periodic investment statements, in and of themselves, do not demonstrate sufficiently continuous ownership of securities. The Staff reiterated that in order to be eligible to submit a shareholder proposal to a company for inclusion in its proxy materials, the "[s]hareholder must submit an affirmative written statement from the record holder of his or her securities that specifically verifies that the shareholder owned the securities *continuously* for a period of one year as of the time of submitting the proposal." Staff Legal Bulletin No. 14 (CF) (July 13, 2001). There is no indication in either the Comerica Letters or the bank statements attached thereto that the AT&T

---

[3] Copies of the six Comerica Letters and their attachments, as submitted by Proponent ADS, are attached to this letter as Appendix 1.

[4] A copy of the deficiency letter, dated November 21, 2007, from AT&T to Proponent ADS is attached to this letter as Appendix 2.

[5] A copy of Proponent ADS's letter, dated November 29, 2007, in response to AT&T's deficiency letter and its attachments is attached to this letter as Appendix 3.

shares in Proponent ADS's accounts have been held continuously from the date of their purchase to the date of the Comerica Letters.

Second, the Comerica Letters are dated as of November 19, 2007 and the attached bank records are dated as of November 15, 2007. The ADS Proposal, however, was submitted no earlier than November 20, 2007. Therefore, neither the Comerica Letters nor the bank records attached thereto clearly indicate that Proponent ADS held the requisite Company shares continuously for one year *as of the date the ADS Proposal was submitted.*

The Staff has previously made clear the need for precision in the context of demonstrating a shareholder's eligibility under Rule 14a-8(b) to submit a shareholder proposal. In Staff Legal Bulletin No. 14, in response to the following question:

> If a shareholder submits his or her proposal to the company on June 1, does a statement from the record holder verifying that the shareholder owned the securities continuously for one year as of May 30 of the same year demonstrate sufficiently continuous ownership of the securities as of the time he or she submitted the proposal?

the Staff replied:

> No. A shareholder must submit proof from the record holder that the shareholder continuously owned the securities for a period of one year as of the time the shareholder submits the proposal.

Staff Legal Bulletin No. 14 (CF) (July 13, 2001). The Staff has previously allowed companies, in much the same circumstances, to omit shareholder proposals pursuant to Rules 14a-8(f) and 14a-8(b) where the proof of eligibility submitted by the shareholder failed to specifically establish that the shareholder held the requisite company stock continuously for one year at the time the proposal was submitted. For example, in International Business Machines Corp., the company argued:

> It is well established that a proposal is considered submitted to a registrant under the proxy rules as of the date such proposal is received by the registrant....While such letter may contain information as of [October 15, 2007], since the Broker's letter was dated four (4) days before the date of the Proponent sent the Proposal to IBM, and, more importantly, seven (7) days before IBM received the Proponent's submission on October 22, 2007, the Broker's Letter did not – and indeed could not – provide any information properly responsive to the Company's written request.

The Staff agreed and permitted the company to omit the shareholder proposal pursuant to Rule 14a-8(f) because the shareholder "failed to supply...documentary support sufficiently evidencing that she satisfied the minimum ownership requirement for the one year period required by [R]ule 14a-8(b)." *International Business Machines Corp.*

(December 7, 2007). See, also, *Eastman Kodak Company* (February 7, 2001); *International Business Machines Corp.* (February 18, 2003); *International Business Machines Corp.* (December 26, 2002); *Gap, Inc.* (March 3, 2003).

Therefore, the documentation submitted by Proponent ADS does not substantiate its eligibility under Rule 14a-8(b), and AT&T can properly exclude the ADS Proposal from its 2008 proxy materials pursuant to Rule 14a-8(f).

Proponent Calvert failed to establish that it has owned its requisite shares of Company stock continuously for one year prior to the date of submission of the Calvert Proposal.

Proponent Calvert submitted the Calvert Proposal to the Company by letter, dated November 20, 2007, along with "supporting documentation" of Proponent Calvert's eligibility to submit the Proposal under Rule 14a-8(b). Enclosed with Proponent Calvert's submission was a letter from State Street Corp. ("State Street") that stated the following: "This letter is to confirm that as of November 15, 2007 the Calvert Funds listed below held the indicated amount of shares of the stock of AT&T, INC. (CUSIP 00206R102). Also the funds held the amount of shares indicated continuously for one year;" the letter also included a table indicating, for each fund, the "shares as of 11/15/07" and the "shares held for 1 year."[6] AT&T received Proponent Calvert's letter on November 21, 2007.

The initial letter from State Street submitted with the Calvert Proposal was deficient in that it failed to establish Proponent Calvert's continuous holding of AT&T stock for at least one year as of the date of submission of the Calvert Proposal.

In accordance with Rule 14a-8(f)(1), AT&T gave timely notice to Proponent Calvert of the requirement to establish eligibility under Rule 14a-8(b) in a letter, dated November 26, 2007. The letter informed Proponent Calvert that the Commission's regulations required it to provide the Company with documentary proof that it owned the requisite amount of Company stock continuously for at least one year prior to submitting its Proposal within 14 days from receipt of the Company's deficiency letter.[7]

In response to the Company's deficiency letter, Proponent Calvert submitted a letter, dated December 6, 2007, attaching a new letter from State Street, identical to the original State Street letter in all respects except that the new letter stated that Proponent Calvert's funds held the shares of AT&T stock "as of November 20, 2007."[8] Proponent Calvert's attempt to remedy the deficiency in its proof of eligibility under Rule 14a-8(b)

---

[6] A copy of the first letter from State Street, dated November 16, 2007, as submitted by Proponent Calvert, is attached to this letter as Appendix 4.

[7] A copy of the deficiency letter, dated November 26, 2007, from AT&T to Proponent Calvert is attached to this letter as Appendix 5.

[8] A copy of Proponent Calvert's letter, dated December 6, 2007, in response to AT&T's deficiency letter, and the attached second letter from State Street, dated December 3, 2007, is attached to this letter as Appendix 6.

nonetheless fails because the new letter from State Street is still fatally defective for two reasons.

First, the new letter from State Street fails to indicate the date as of which Proponent Calvert held the requisite amount of AT&T stock continuously for one year. As discussed more fully in respect to the ADS Proposal above, the proponent must submit an affirmative written statement from the record holder of his or her securities that specifically verifies that the shareholder owned the securities continuously for a period of one year as of the time of submitting the proposal. The new letter states only that Proponent Calvert's "funds held the amount of shares indicated continuously for one year." However, it does not indicate the date as of which such shares were held. Moreover, the letter includes two distinct columns: one labeled "shares as of 11/20/07" and the other labeled "shares held for one year." Again, however, the column labeled "shares held for one year" does not indicate the date as of which such shares were held. These statements indicate that Proponent Calvert held its AT&T shares for one continuous year at some point since the time they were purchased, but they do not establish that the one year continuous holding period was as of the date of submission of the Calvert Proposal. For instance, these statements may speak as of the date of the new letter from State Street – December 3, 2007 – rather than as of the date the Calvert Proposal was submitted. Therefore, the new letter from State Street fails to specifically verify that Proponent Calvert owned the requisite securities continuously for a period of one year *as of the time of submitting the Calvert Proposal.*

Second, the date on which the requisite shares were owned, as indicated in the new State Street letter, does not correspond to the date of submission of the Calvert Proposal. Although, as discussed above, the new State Street letter does not indicate the date as of which the requisite shares were held continuously for one year, it does indicate the number of shares owned on November 20, 2007. However, submission occurs when a company actually receives the proposal, not when the proponent mails or otherwise delivers it. Thus, the November 20, 2007 date referenced in the new letter from State Street does not correspond to the date the Calvert Proposal was submitted – November 21, 2007.[9] As discussed more fully with respect to the ADS Proposal above, the Staff has already explicitly addressed the need for precision in demonstrating a shareholder's eligibility under Rule 14a-8(b). Therefore, the new letter from State Street does not indicate that Proponent Calvert owned the requisite shares

[9] The principle that a shareholder proposal is considered submitted to a company under the proxy rules as of the date such proposal is received by the company is well established. Rule 14a-8(e) provides that submission of a shareholder proposal is calculated as of the date the proposal is received at the company's principal executive offices. See also, *International Business Machines Corp.* (December 7, 2007) (discussed above); *Agere Systems Inc.* (November 16, 2005); *Merrill Lynch & Co., Inc.* (December 30, 2004) (in both cases, the Staff permitted exclusion under Rule 14a-8(e) because the shareholder proposal was not received by the company within the requisite time period).

at all, much less continuously for a period of one year, as of the date that the Calvert Proposal was submitted.

Therefore, the documentation submitted by Proponent Calvert does not substantiate its eligibility under Rule 14a-8(b), and AT&T can properly exclude the Calvert Proposal from its 2008 proxy materials pursuant to Rule 14a-8(f).

The Proposals May be Omitted from the Proxy Statement Pursuant to Rule 14a-8(i)(2): Implementation of the Proposals by the Company 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 Proposals is that AT&T has provided certain customer information to the NSA and that such action constitutes a violation of law and the privacy rights of AT&T customers. Although the Supporting Statements provide that the required report may be prepared by the Board "without necessarily referring to any specific program," the type of report mandated by the Proposals would clearly encompass a discussion of AT&T's alleged cooperation with government agencies, including the NSA, and would, at least implicitly, require the Company to provide information that would confirm or deny such cooperation. AT&T has obtained a legal opinion from the law firm of Sidley Austin LLP (the "Sidley Austin Opinion") which describes in detail the laws governing the disclosure of the alleged activities involving the NSA and other government agencies.[10] The Sidley Austin Opinion confirms that it would be impossible for AT&T to produce the report called for by the Proposals, without providing information which the United States has deemed classified and over which it has asserted its state secrets privilege. Therefore, according to the Sidley Austin Opinion, implementing the Proposals 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. However, if the Board were to exclude all classified information from the required report, along with all of the other types of information permitted to be excluded by the Proposals, the report would contain no substantive information and would thus defeat the purpose of the Proposals.

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 Proposals would violate federal law, AT&T can exclude the Proposals from its 2008 proxy materials in accordance with Rule 14a-8(i)(2).

---

[10] The Sidley Austin Opinion is attached to this letter as Appendix 7.

The Proposals May be Omitted from the Proxy Statement Pursuant to Rule 14a-8(i)(7): The Proposals relate 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 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).[11]

The Proposals relate to ongoing litigation involving the Company.

The Proposals may be omitted pursuant to Rule 14a-8(i)(7) as a matter involving ordinary business because they improperly interfere with the Company's legal strategy and the discovery process in at least 20 pending proceedings that allege unlawful acts by AT&T in relation to alleged provision of customer information to the NSA.

AT&T is presently the defendant in multiple pending lawsuits and other proceedings that generally allege that AT&T has violated customer privacy rights by providing information and assistance to government entities without proper legal authority, including allegedly providing information to the NSA. For example, in Terkel & American Civil Liberties Union of Illinois v. AT&T, plaintiffs alleged that AT&T has provided the NSA 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. *Terkel & American Civil Liberties Union of Illinois v. AT&T,* No. 06 C 2837 (N.D. Ill.). Similarly, these same allegations were also made in Hepting v. AT&T, where the plaintiffs also alleged that AT&T had acted unlawfully by providing the NSA with the contents of customer communications in the absence of a court order, warrant, or certification from the Attorney General that no such process was required. *Hepting v. AT&T,* No. 3:06-CV-006720-VRW (N.D. Cal.). There are over 20 pending cases that

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

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 American Civil Liberties Union (the "ACLU")[12] have filed complaints with over 20 state regulatory bodies 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 regulatory body 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.[13]

The Proposals call for a report discussing "the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosure on privacy rights of customers." The need for this report, Proponents argue in the Supporting Statements, "is particularly acute in the wake of reports that AT&T voluntarily, and without a warrant, provided customer phone records and communications data to the National Security Agency." Thus, the Proposals call for the same information that the plaintiff ACLU and others seek in discovery and thereby sidesteps and interferes with the discovery process. By requiring the Board to provide this exact information in a report to shareholders, the Proposals essentially do away with the discovery process and can therefore be properly omitted as improperly interfering with the ordinary business of the Company's conduct of its ongoing litigation matters. In fact, as already mentioned above, the Staff has already excluded a substantially similar proposal, co-sponsored by Proponents, on this very ground. See *AT&T Inc.* (February 9, 2007).

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 company 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

---

[12] We note that on the ACLU website, it claims responsibility for "The ACLU Freedom Files," a television series, co-executive produced and directed by Jeremy Kagan, which, 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 to the episode entitled "Beyond the Patriot Act," the ACLU repeats the allegation that "Americans' phone calls and e-mails [are monitored] – without court approval." The ACLU Freedom Files Producers Club Viewer Guide, http://www.aclu.tv/system/files/patriotviewersguide.pdf (last visited December 4, 2007). Proponents now seek the same information through the shareholder approval process that the ACLU has sought through litigation.

[13] See *United States* v. *Rabner, 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. *Gaw, et al.*, C.A. 4:06-1132 (E.D. Mo); *United States* v. *Volz, et al.*, C.A. 2:06-00188 (D. Vt.).

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 excluded as ordinary business.); *R. J. Reynolds Tobacco Holdings, Inc.* (February 6, 2004) (proposal requiring the 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 was excluded under the ordinary course of business exception because it interfered with the litigation strategy of a class-action lawsuit on similar matters involving the company); *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 was excluded under the ordinary course of business exception because it related to the subject matter of litigation in which the company was named as a defendant).

This result is also consistent with the Staff's longstanding position that a company's decision to institute or defend itself against legal actions and its 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 the company to bring an action against certain persons was excluded as ordinary business operations because it related to litigation strategy); *Microsoft Corporation* (September 15, 2000) (proposal asking the company to sue the federal government on behalf of shareholders was excluded as ordinary business because it related to the conduct of litigation); *Exxon Mobil Corporation* (March 21, 2000) (proposal requesting immediate payment of settlements associated with the Exxon Valdez oil spill was excluded because it related to litigation strategy and related decisions); *Philip Morris Companies Inc.* (February 4, 1997) (proposal recommending that the company voluntarily implement certain FDA regulations while simultaneously challenging the legality of those regulations was excluded under the ordinary course of business exception); *Exxon Corporation* (December 20, 1995) (proposal requiring the company to forego any appellate or other rights that it might have in connection with litigation arising from the Exxon Valdez oil spill was excluded because the Staff reasoned that a company's litigation strategy and related decisions are matters relating to the conduct of its ordinary business operations).

Even though the Proposals allow the Board to exclude from the required report "information that would reveal the Company's litigation...strategy," the subject matter of the Proposals is nonetheless clearly "the same as or similar to that which is at the heart of" numerous legal proceedings in which AT&T is currently involved. Furthermore, while certain information might not necessarily reveal AT&T's litigation strategy (and thus not be eligible for the permitted exclusion), the provision of such information nevertheless sidesteps and interferes with the discovery process in such litigation. If, on the other hand, the Board were to exclude all such information from the report on the basis that it does reveal AT&T's litigation strategy, along with all of the other types of information permitted to be excluded by the Proposals, the required report would contain no substantive information and would thus defeat the stated purpose of the Proposals.

In effect, the Proposals recommend that AT&T facilitate the discovery of the opposing parties in these various lawsuits at the same time it is challenging those parties' legal positions or claims. Compliance with the Proposals would improperly interfere with AT&T's litigation strategy in these cases and intrude upon management's appropriate discretion to conduct the Company's litigation as its business judgment dictates in the ordinary course of its day-to-day business operations.

The Proposals relate to matters of customer privacy.

The Proposals can be excluded under Rule 14a-(8)(i)(7)'s ordinary business exclusion because they impermissibly seek to subject AT&T's policies and procedures for protecting customer information to shareholder oversight. The development and implementation of such policies and procedures is an integral part of AT&T's day-to-day business operations and a function that is most appropriately left to the discretion of management.

The Staff has long recognized that the protection of customer privacy is a core management function, not subject to shareholder oversight, and has, to that end, allowed companies to exclude proposals requesting reports on issues related to customer privacy. In Verizon Communications Inc., a shareholder submitted a proposal substantially similar to the Proposals in this case, requesting that the company prepare a report describing "the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content" to government and non-government agencies, including the NSA. The Staff allowed Verizon to exclude the proposal from its proxy materials on the ground that it related "to Verizon's ordinary business operations (i.e., procedures for protecting customer information)." *Verizon Communications Inc.* (February 22, 2007).

Similarly, 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) (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) (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); *Citicorp* (January 8, 1997) (proposal requesting the company to prepare a report on policies and procedures to monitor illegal transfers through customer accounts was excluded under the ordinary business exclusion).

The Proposals are virtually identical to the Verizon and Bank of America proposals in that they request AT&T to produce a report addressing its policies for disclosing customer information to federal and state agencies and the effect of such disclosure on customer privacy, in response to a perceived breach of that privacy. Thus, the Proposals explicitly deal with matters of customer privacy and the Company's policies and procedures for protecting customer information. As the Staff has already recognized, these matters are integral to the day-to-day business operations of a company and cannot, "as a practical matter, be subject to direct shareholder oversight." As such, the Proposals should be omitted from AT&T's 2008 proxy materials because they impermissibly subject this integral part of the Company's business operations to shareholder oversight.

The Proposals relate to matters of legal compliance.

The Proposals can also be properly excluded, pursuant to Rule 14a-8(i)(7), because they seek 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) (proposal requesting the company to prepare a report detailing its environmental protection and pollution control activities was excluded as relating to the ordinary business of complying with government regulations); *Halliburton Company* (March 10, 2006) (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) (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).

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."

The essence of the Proposals 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 Proposals look for the technical, legal and policy issues related to the Company's cooperation with federal and state agencies and the effect that such

cooperation may have on its customers. The information requested by the Proposals 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.

If, on the other hand, in preparing the required report the Board were to exclude all such information as information revealing the Company's compliance strategy, along with the other types of information also permitted to be excluded by the Proposals, then the required report would contain no substantive information and would thus defeat the purpose of the Proposals.

The Proposals involve the Company in the political or legislative process.

AT&T believes that exclusion of the Proposals is justified because the Proposals involve 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 Proposals essentially request AT&T to evaluate the impact that the alleged government surveillance programs would have on the Company's business operations, including the effect on the privacy rights of its customers. In this way, the Proposals can be seen as involving AT&T in the political process, and, therefore, excludable as relating to the Company's ordinary business.

The Proposals can be excluded as relating to matters of ordinary business, regardless of whether or not they touch upon a significant public 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 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) (in both cases, excluding proposals requesting inward-looking reports on the economic effects of HIV/AIDS, tuberculosis and malaria

pandemics on the company's business strategies and risk profiles). The Proposals fall squarely in this group.

The Proposals request that the Board issue a report on matters relating to AT&T's ordinary business and, as such, may be properly omitted pursuant to Rule 14a-8(i)(7).

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

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 Proposals, by their own terms, are inherently contradictory - according to the Proposals, AT&T is, at the same time, required to provide information and permitted to exclude the same information. The Proposals call for a report discussing "the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies" but allows the Board in preparing this report to specifically exclude "proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying efforts." As discussed in the previous sections of this letter, virtually all of the substantive information required by the Proposals to be included in the report falls into at least one, if not all, of the categories of information which the Proposals themselves explicitly allow to be excluded from the same report. The Sidley Austin Opinion confirms that the essential portion of the information requested by the Proposals, if it existed, would be identified by the United States as classified information and must be treated confidentially.[14] Furthermore, the requested information, as discussed above, would also reveal AT&T's regulatory and litigation strategy. These conflicting mandates make the Proposals inherently vague and indefinite and, as such, impossible for AT&T to implement. Therefore, the Proposals 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) (resolution that a committee of small stockholders refer a "plan or plans" to the company's board of directors without describing the substance of those plans was omitted under predecessor Rule 14a-8(c)(3)); *Johnson & Johnson* (February 7, 2003) (permitting omission of proposal calling for a report on the company's "progress with the Glass Ceiling Report," but not

[14] For further analysis, refer to the Sidley Austin Opinion.

explaining the substance of the report); *H.J. Heinz Co.* (May 25, 2001) and *Kohl's Corp.* (March 13, 2001) (in both cases, proposals were excluded under Rule 14a-8(i)(3) because they requested the company to implement the SA8000 Social Accountability Standards, but did not clearly set forth what SA8000 required of the company). 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, the proposal is "beyond the [company's] power to effectuate." *Int'l Business Machines Corporation* (January 14, 1992); see also, *The Southern Company* (February 23, 1995) (permitted the exclusion of 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 all of the substantive information required by the Proposals is either confidential, classified or would reveal the Company's litigation or regulatory strategy, the Proposals essentially request AT&T to produce a report excluding the very substance of the required report. Thus, the terms of the Proposals 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 Proposals. As such, the Proposals, if adopted, would be beyond AT&T's "power to effectuate." If AT&T were to implement the Proposals as drafted, it would issue a report excluding substantially all of the information sought by the Proposals. Since the Supporting Statements make clear that the Proposals seek to require AT&T to "provide a clear statement" on its policies for disclosing customer information to federal and state agencies, implementing the Proposals, as drafted, would essentially defeat the very purpose of the Proposals and would thus result in a significantly different outcome than that envisioned by the shareholders voting on the Proposals.

Because the terms of the Proposals are inherently vague and indefinite, AT&T believes that it can properly omit the Proposals from its 2008 proxy materials under Rules 14a-8(i)(3) and 14a-8(i)(6).

The Proposals May be Omitted from the Proxy Statement Pursuant to Rule 14a-8(i)(10): The Proposals have been substantially implemented.

The Proposals may also be omitted from the 2008 proxy materials because AT&T believes that, insofar as it is able to do so consistent with federal law, it has already

substantially implemented the Proposals by satisfactorily addressing its underlying concerns in its Privacy Policy, which is publicly available to shareholders on AT&T's website.

Rule 14a-8(i)(10) permits a company to omit a shareholder proposal if it has already been substantially implemented by the company. The substantially implemented standard reflects the Staff's interpretation of the predecessor rule allowing the omission of a "moot" proposal: in order to properly exclude a shareholder proposal under Rule 14a-8(i)(10) as "moot," the proposal does not have to be "fully effected" by the company so long as the company can show that it has "substantially implemented" the proposal. Exchange Act Release No. 34-20091 (August 16, 1983). The determination of whether a company has satisfied the "substantially implemented" standard "depends upon whether [the company's] particular policies, practices and procedures compare favorably with the guidelines of the proposal." *Texaco, Inc.* (March 28, 1991). Moreover, the Staff has consistently allowed for the exclusion of shareholder proposals as substantially implemented where a company already has polices and procedures in place relating to the subject matter of the proposal. See, e.g. *The Gap, Inc.* (March 16, 2001) (proposal asking the company to prepare a report on the child labor practices of its suppliers was excluded as substantially implemented by the company's code of vendor conduct, which was discussed on the company's website); *Nordstrom Inc.* (February 8, 1995) (proposal that the company commit a code of conduct for overseas suppliers was excluded as substantially covered by the company's existing guidelines).

The Staff has also established that a company does not have to implement every detail of a proposal in order to exclude it under Rule 14a-8(i)(9). Rather, "substantial implementation" requires only that the company's actions "satisfactorily address the underlying concerns of the proposal." *Masco Corp.* (March 29, 1999); see also, *Entergy, Inc.* (January 31, 2006) (the Staff excluded proposal to adopt a "simple majority vote" on issues subject to shareholder vote on the ground that the company had substantially implemented the proposal when it amended its bylaws to have the same effect as the proposal).

The underlying concern of the Proposals is summed up in the last sentence of the Supporting Statements: "We therefore believe that AT&T should, without necessarily referring to any specific program, report to shareholders as the Company's policy with respect to requests for warrantless access to information about AT&T customers." In fact, AT&T's Privacy Policy, which is available on the Company's website at http://att.com, already covers the Company's current policies, practices and procedures for protecting the confidentiality of customer information, including what customer information is collected and how it can be used, when and to whom it may be disclosed (including to law enforcement and other government agencies) and how the Company implements and updates its privacy policies, practices and procedures.[15]

[15] A copy of AT&T's Privacy Policy is also attached to this letter as Appendix 8.

Therefore, AT&T believes that the Proposals may be omitted from its proxy materials pursuant to Rule 14a-8(i)(10) because it has already developed, executed and made publicly available a comprehensive Privacy Policy that "compares favorably with the guidelines of the" Proposals and that substantially addresses the Proposals' underlying concern.

* * *

For the reasons set forth above, we ask the Staff to recommend to the Commission that no action be taken if the Proposals are omitted from AT&T's 2008 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.

Sincerely,

Paul Wilson
Senior Attorney

Enclosures

cc: Jonas D. Kron, Attorney at Law
Sister Annette M. Sinagra, OP, Corporate Responsibility Analyst of the Adrian Dominican Sisters
Aditi Vora, Social Research Analyst, Calvert Asset Management Company, Inc.

Appendix 1

3

Comerica Bank

Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
T ROWE PRICE VALUE
Account# *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 27,264 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

5

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
T ROWE PRICE GROWTH
Account# *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 1,900 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
ATALANTA SOSNOFF CAPITAL
Account *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 10,200 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

9

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
ATALANTA SOSNOFF CAPITAL PATRIMONY
Account *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 2,250 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

//

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
PATRIMONY – TRUST COMPANY OF THE WEST
Account# *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 4,250 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
EQUITY– TRUST COMPANY OF THE WEST
Account# *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 8,600 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

Appendix 2

Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
175 E. Houston, Room 216
San Antonio, Texas 78205
Ph. (210) 351-3407

November 21, 2007

Via UPS
Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
Adrian Dominican Sisters
Human Resources Department
1257 East Siena Heights Drive
Adrian, Michigan 49221-1793

Dear Sr. Sinagra:

Today we received your faxed letter dated November 15, 2007, submitting a stockholder proposal on behalf of the Adrian Dominican Sisters for inclusion in AT&T Inc.'s 2008 Proxy Statement. We are currently reviewing the proposal to determine if it is appropriate for inclusion in our 2008 Proxy Statement.

Under the rules of the Securities and Exchange Commission ("SEC"), in order to be eligible to submit a stockholder proposal, a stockholder must: (a) be the record or beneficial owner of at least $2,000 in market value of the common stock of AT&T Inc. at the time a proposal is submitted, and (b) have continuously owned these shares for at least one year prior to submitting the proposal. Therefore, in accordance with the rules of the SEC, please provide us with documentary support that all of the above-mentioned requirements have been met.

For shares registered in your name, you do not need to submit any proof of ownership since we will check the records of AT&T's transfer agent. For shares held by a broker, the *broker* must provide us with a written statement as to when the shares were purchased and that the minimum number of shares have been continuously held for the one year period. *You must provide the documentation specified above, and your response must be postmarked or electronically transmitted, no later than 14 days from your receipt of this letter.*

Please note that if you or your qualified representative does not present the proposal at the meeting, it will not be voted upon. The date and location for the 2008 Annual Meeting of Stockholders will be provided to you at a later date.

Sincerely,

Nancy H. Justice

Appendix 3

ADRIAN DOMINICAN SISTERS
1257 East Siena Heights Drive
Adrian, Michigan 49221-1793
517-266-3522 Phone
517-266-3524 Fax

Portfolio Advisory Board

November 26, 2007

Ms. Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
175 E. Houston - Room 216
San Antonio, TX 78205

Dear Ms. Justice:

Enclosed you will find a copy of my filing letter, the shareholder resolution we presented to AT&T and letters from our holding bank stating our ownership of AT&T stock.

Thank you for attending to this matter.

Sincerely,

Sister Annette M. Sinagra, O.P.

Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
Adrian Dominican Sisters

ADRIAN DOMINICAN SISTERS
1257 East Siena Heights Drive
Adrian, Michigan 49221-1793
517-266-3522 Phone
517-266-3524 Fax
ASinagra@adriandominicans.org
Portfolio Advisory Board

VIA FAX: 210/351-3467

November 15, 2007

Mr. Wayne Wirtz
Assistant General Counsel
AT&T Inc.
175 E. Houston Street
P.O. Box 2933
San Antonio TX 78299-2933

The Adrian Dominican Sisters are the beneficial owners of 54,464 shares of common stock in AT&T, INC. Letters of stock verification are enclosed. Ownership of our shares will continue through the dated of the company's next annual meeting. As a representative of the Adrian Dominican Sisters, I am authorized to notify you of our intention to submit the enclosed resolution entitled: *Privacy Rights Report,* for consideration and action by shareholders at AT&T, INC's next annual meeting. We are co-sponsors with As You Sow, the primary sponsor. Other members of the interfaith Center on Corporate Responsibility may also submit filings of the enclosed resolution.

As a representative of the Adrian Dominican Sisters, I am authorized to notify you of our intention to submit the enclosed resolution entitled: *Privacy Rights Protection Report,* for consideration and action by shareholders at AT&T's next annual meeting. We will hold our shares in the company until after this meeting. We are co-sponsors of this resolution in conjunction with As You Sow, the primary filer. Other member of the Interfaith Center on Corporate Responsibility may co-sponsor this resolution as well. Therefore, I submit it for inclusion in the proxy statement in accordance with rule 14a-8 of the general rules and regulations of the security Act of 1934. We request that the Adrian Dominican Sisters be named as co-sponsors of this resolution when the company prepares its proxy materials for the next annual meeting.

Since I am faxing this filing, our institution would appreciate your sending an e-mail confirmation that all the documentation was received. My e-mail address is included below for your convenience. We are available for future dialogue as the season progresses regarding the content of the resolution.

Sincerely,

Sister Annette M. Sinagra, OP

Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
asinagra@adriandominicans.org

cc:
Mr. Edward E. Whitacre Jr.
Chairman & CEO
AT&T Inc.

AT&T INC.-2007
PRIVACY RIGHTS PROTECTION REPORT

RESOLVED: The shareholders of AT&T (the "Company") hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. The report should be prepared at reasonable cost and made available to shareholders within six months of the annual meeting, and it may exclude proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy.

SUPPORTING STATEMENT

The right to privacy is a long-established value, embedded in the Constitution and decades of U.S. jurisprudence, and cherished by people of all political persuasions. Privacy protections serve many important societal purposes: encouraging development of science and knowledge; preventing fraud; and allowing individuals to communicate sensitive personal information (e.g., to health care providers and clergy).

AT&T states that it is committed to the highest standards of ethics, integrity, and personal and corporate responsibility. We believe these high standards make it incumbent on AT&T to not undermine privacy rights, but rather to conduct itself in support of this American tradition of liberty which is at the foundation of our nation, democracy and basic human rights.

AT&T's reputation and good standing can be adversely affected by the perception that the Company is not adequately protecting the privacy of its customers. In our view, this threat is particularly acute in the wake of reports that AT&T voluntarily, and without a warrant, provided customer phone records and communications data to the National Security Agency.

Since reports of this cooperation first surfaced over a year ago, there have been numerous media stories, as well as public debate, on the topic. We believe that disclosure of sensitive records without a warrant is viewed by millions of Americans as, if not unlawful, then at least a violation of a customer's expectations of having telephone and e-mail records kept confidential. Telecommunications customers have choices in the marketplace and can take their business to other firms if they believe that the Company is insufficiently sensitive to these issues.

We therefore believe that AT&T should, without necessarily referring to any specific program, report to shareholders as to the Company's policy with respect to requests for warrantless access to information about AT&T customers. In our view, being able to provide a clear statement on this subject in an era of rapidly evolving technology, presents an opportunity for AT&T to play a leadership role in the protection of customer privacy rights, for the benefit of shareholders.

We urge you to vote FOR this resolution in support of privacy rights protection.

3

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
T ROWE PRICE VALUE
Account# *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 27,264 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

6

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
T ROWE PRICE GROWTH
Account # *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 1,900 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

7

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
ATALANTA SOSNOFF CAPITAL
Account *** SMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 10,200 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

Y

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
ATALANTA SOSNOFF CAPITAL PATRIMONY
Account *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 2,250 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

11

Comerica Bank
Wealth & Institutional Management

Comerica Bank

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
PATRIMONY – TRUST COMPANY OF THE WEST
Account *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 4,250 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

November 19, 2007

Margaret Weber
Coordinator of Corporate Responsibility
Adrian Dominican Sisters
1257 E. Siena Hts. Drive
Adrian, MI 49221

RE: ADRIAN DOMINICAN SISTERS
EQUITY– TRUST COMPANY OF THE WEST
Account *** FISMA & OMB Memorandum M-07-16 ***

Dear Margaret:

In regard to your request for a verification of holdings, the above referenced account currently holds 8,600 shares of AT & T, common stock. The attached list indicates the date the stock was acquired.

Please feel free to contact me should you have any additional questions or concerns.

Sincerely,

Norma Batson
Account Analyst
1-313-222-5757
Norma_J_Batson@Comerica.com

Enclosure

*** FISMA & OMB Memorandum M-07-16 ***

Appendix 4

STATE STREET.

Investment Services
P.O. Box 5607
Boston, MA 02110

November 16, 2007

Calvert Group, LTD
Fund Administration
4550 Montgomery Avenue, Suite 1000N
Bethesda, MD 20814

To Whom It May Concern:

This letter is to confirm that as of November 15, 2007 the Calvert Funds listed below held the indicated amount of shares of the stock of AT&T, INC. (CUSIP 00206R102). Also the funds held the amount of shares indicated continuously for one year.

Fund Number	Name	Shares as of 11/15/07	Shares held for 1 year
	CSIF Balanced Portfolio	260,165	244,965
*** FISMA & OMB Memorandum M-07-16 ***	CVS Calvert Social Balanced Portfolio	211,277	198,577
	CSIF Enhanced Equity Portfolio	80,842	61,838
	Calvert Social Index Fund	70,459	62,176

Please feel free to contact me if you need any further information.

Sincerely,

Michelle McElroy

Michelle McElroy
Account Manager
State Street Corp

Appendix 5

Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
175 E. Houston, Room 216
San Antonio, Texas 78205
Ph. (210) 351-3407

November 26, 2007

Via UPS
William M. Tartikoff, Esq.
Vice President and Secretary
Calvert Asset Management Company, Inc.
4550 Montgomery Avenue
Bethesda, MD 20814

Dear Mr. Tartikoff:

On November 21, 2007, we received your letter dated November 20, 2007, submitting a stockholder proposal on behalf of Calvert Asset Management Company, Inc. for inclusion in AT&T Inc.'s 2008 Proxy Statement. We are currently reviewing the proposal to determine if it is appropriate for inclusion in our 2008 Proxy Statement.

Under the rules of the Securities and Exchange Commission ("SEC"), in order to be eligible to submit a stockholder proposal, a stockholder must: (a) be the record or beneficial owner of at least $2,000 in market value of the common stock of AT&T Inc. at the time a proposal is submitted, and (b) have continuously owned these shares for at least one year prior to submitting the proposal. Therefore, in accordance with the rules of the SEC, please provide us with documentary support that all of the above-mentioned requirements have been met.

For shares registered in your name, you do not need to submit any proof of ownership since we will check the records of AT&T's transfer agent. For shares held by a broker, the *broker* must provide us with a written statement as to when the shares were purchased and that the minimum number of shares have been continuously held for the one year period. *You must provide the documentation specified above, and your response must be postmarked or electronically transmitted, no later than 14 days from your receipt of this letter.*

Please note that if you or your qualified representative does not present the proposal at the meeting, it will not be voted upon. The date and location for the 2008 Annual Meeting of Stockholders will be provided to you at a later date.

Sincerely,

Nancy H. Justice

Appendix 6

Calvert
INVESTMENTS
THAT MAKE A DIFFERENCE®

December 6, 2007

Via Facsimile and Overnight
Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
175 E. Houston, Room 216
San Antonio, Texas 78205

Dear Ms. Justice,

I am writing in response to your November 26, 2007 letter to William M. Tartikoff regarding the stockholder proposal submitted by Calvert Asset Management Company, Inc. stockholder proposal.

Please see the enclosed letter documenting that the Calvert Social Index Fund, the Calvert Social Investment Fund, Balanced Portfolio, the Calvert Variable Series, Inc., Calvert Social Balanced Portfolio, and the Calvert Social Investment Fund Enhanced Equity Portfolio each held more than $2,000 in market value of AT&T Inc. common stock as of close of business on November 20, 2007 when Calvert submitted its shareholder proposal, and that each of these funds has continuously held these shares for at least one year prior to the date we submitted the proposal.

Please contact me immediately by phone at (301)-961-4762 or email stu.dalheim@calvert.com if you have any further questions regarding this matter.

Sincerely,

Stu Dalheim
Manager of Advocacy and Policy
Calvert Group, Ltd.

Enclosures:
State Street Letter

4550 Montgomery Avenue
Bethesda, MD 20814
301.951.4800
www.calvert.com
A UNIFI Company.

STATE STREET.

Investment Services
P.O. Box 5607
Boston, MA 02110

December 3, 2007

Calvert Group, LTD
Fund Administration
4550 Montgomery Avenue, Suite 1000N
Bethesda, MD 20814

To Whom It May Concern:

This letter is to confirm that as of November 20, 2007 the Calvert Funds listed below held the indicated amount of shares of the stock of AT&T, INC. (CUSIP 00206R102). Also the funds held the amount of shares indicated continuously for one year.

Fund Number	Name	Shares as of 11/20/07	Shares held for 1 year
*** FISMA & OMB Memorandum M-07-16 ***	CSIF Balanced Portfolio	260,165	244,965
	CVS Calvert Social Balanced Portfolio	211,277	198,577
	CSIF Enhanced Equity Portfolio	80,842	61,838
	Calvert Social Index Fund	70,459	66,423

Please feel free to contact me if you need any further information.

Sincerely,

Michelle McElroy

Michelle McElroy
Account Manager
State Street Corp

Appendix
7

SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
ONE SOUTH DEARBORN
CHICAGO, IL 60603
(312) 853 7000
(312) 853 7036 FAX

BEIJING
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
LONDON

LOS ANGELES
NEW YORK
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

December 6, 2007

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

Re: Shareholder Proposal

Ladies and Gentlemen:

You have requested our legal opinion whether it would violate federal law for AT&T Inc. ("AT&T" or the "Company") to implement a shareholder proposal that has been submitted by the Adrian Dominican Sisters and Calvert Asset Management Company, Inc. (the "Proposal") for inclusion in the Company's next proxy statement.[1]

The Proposal. The proposed resolution calls for the AT&T Board of Directors to issue a report to shareholders describing, *inter alia,* "from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers." The Proposal states that such report "may exclude proprietary, classified, and confidential information, including information that would reveal the Company's litigation, regulatory, or lobbying strategy."

In the Supporting Statement, the proponents state that the right to privacy is of great importance and that "AT&T's reputation and good standing can be adversely affected by the perception that [it] is not adequately protecting privacy rights." The proponents state that this concern is "particularly acute" because of the newspaper reports that "AT&T voluntarily, and without a warrant, provided customer phone records and communications data to the National Security Agency [(the "NSA")]." The proponents are here referring to the May 11, 2006, *USA Today* article that reported that AT&T and other carriers were providing NSA with all their

[1] The Proposal and cover letter are attached hereto as Exhibit 1. We note that, by our letter of November 22, 2006, we provided our legal opinion regarding a similar shareholder proposal submitted by Jeremy Kagan along with several co-filers on October 24, 2006 to AT&T Inc. for inclusion in its proxy statement. Our analysis of this new Proposal is independent of our analysis of the prior proposal, although we reach the same conclusion.

customers' calling records for use in NSA's counterterrorism activities ("the Calling Records Program")[2] and to the reports that AT&T and other carriers have enabled NSA to obtain the contents of all voice and email communications carried over AT&T's network (the "Terrorist Surveillance Program.").[3] The United States has neither confirmed nor denied either the existence of a Calling Records Program or the participation of any individual carriers in it. While the United States has confirmed the existence of a Terrorist Surveillance Program in which it intercepts the contents of certain international telephone calls involving suspected al Qaeda agents, it has not confirmed or denied whether particular carriers are participating in the program, and it has stated that all other details regarding the operation of this program are classified.[4] This letter will refer to the Terrorist Surveillance Program and the alleged Calling Records Program collectively as the "Program" or the "Programs."

The proponents of the Proposal state that there has been a "public debate" on the propriety of warrantless access to such information in the period "[s]ince reports of this cooperation first surfaced over a year ago" and that they believe that "disclosure of sensitive records without a warrant is viewed by millions of Americans as, if not unlawful, at least a violation of a customer's expectations of having telephone and email records kept confidential." The proponents state that if AT&T is "insufficiently sensitive to these issues," customers "can take their business to other firms."

For these reasons, the proponents propose that "AT&T should, without necessarily referring to any specific program, report to shareholders as to the Company's policy with respect to requests for warrantless access to information" and that AT&T play a "leadership role" by providing a "clear statement" on the "protection of customer privacy rights" in an era of rapidly evolving technology.

Thus, the instant Proposal is that AT&T prepare a report that addresses all the conditions in which it does and does not provide information or assistance to state or federal agencies in the absence of warrants and that "clearly state[s]" whether and how AT&T protects customers privacy rights when confronted with such requests – without "necessarily" addressing specific programs.

---

[2] *See* Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2006, at A1.
[3] *See* James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, Dec. 16, 2005, at A1.
[4] *See* Press Conference of President Bush (Dec. 19, 2005), available at http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html; and 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.

Analysis. AT&T cannot legally provide the proposed report. Whether or not the report expressly discussed the alleged NSA Calling Records program or any other specific program, any such report would have to include analyses of any requests for assistance that have, or have not, been made by federal agencies charged with protecting national security and of the actions that AT&T has, or has not, taken in response to such requests. Because this is classified information and covered by the Government's assertion of the federal state secrets privilege, federal law prohibits AT&T from preparing the requested report.

In this regard, the instant Proposal is legally indistinguishable from the investigations that a number of state officials sought to initiate in the aftermath of the May 11, 2006 *USA Today* article. There, as here, each proceeding was initiated in response to the allegations that AT&T was providing calling records and other information to NSA. There, as here, the proponents of the state investigations frequently stated that they were not interested in learning the details of specific programs but only wanted to ascertain whether and under what conditions AT&T provides information to state and federal agencies in the absence of warrants, court orders, subpoenas, and other such legal authorizations. But in each proceeding, the United States Department of Justice explained that providing the requested information would give the nation's enemies valuable insights into the nation's intelligence gathering operations and that federal law prohibited AT&T from providing the requested information.

For example, shortly after the *USA Today* article appeared, the New Jersey Attorney General attempted to subpoena information relating to whether AT&T had provided calling records to NSA. On June 14, 2006, 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."[5] 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. The United States Department of Justice made the same or similar statements to carriers and to state officials when similar investigations were proposed in Maine, Michigan, Nebraska, Vermont, and Connecticut, and each of the prohibitions referred to in these letters is fully applicable here.

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:

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

> 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.[6]

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 the United States Justice Department advised the Attorney General of New Jersey:

---

[6] 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.*

> 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."[7]

Letter from Assistant Attorney General Peter Keisler to New Jersey Attorney General Zulimna Farber, at 4 (June 14, 2006) (Exhibit 5).[8]

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 government. *See* note 8.

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. Negroponte, ¶ 11 (Exhibit 3).[9] As Director Negroponte stated, "[m]y assertion of the state

---

[7] *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 4).

[8] *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. . . .").

[9] 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*,

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.[10] As noted, the United States has formally directed that AT&T may not publicly disclose any responsive information concerning the claimed Programs. Furthermore, the United States District Court for the District of Columbia has held that even basic numerical or statistical information about the Terrorist Surveillance Program was and remains classified and therefore exempt from disclosure under 5 U.S.C. § 552(b)(1) of the Freedom of Information Act. *People for the American Way Foundation v. NSA et al.*, Civil Action No. 06-206 (ESH) (Nov. 20, 2006), 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 challenges to the United States' assertion that information pertaining to the Programs is classified.[11]

The subjects covered by the criminal prohibition on disclosure of communications intelligence are thus the same subjects which the Proposal concerns. For instance, assuming

---

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).

[10] 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 Negroponte, 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.*

[11] In MDL 06-1791 VRW: *In re National Security Agency Telecommunications Records Litigation*, District Judge Walker preliminarily addressed some of these issues in an Order dated July 27, 2007. He there denied the motion of the United States for summary judgment on its claim that 18 U.S.C. § 798 prevented state commissions from investigating whether carriers have provided calling records to the NSA because he concluded that there had not been a showing that the United States had "specifically designated" the information at issue to be "classified." *Id.* at 26-27. Even then, he concluded that the United States would be entitled to summary judgment if it established that the information is protected by the state secrets privilege, which is an issue that Judge Walker deferred addressing until the Ninth Circuit decides a pending appeal involving Judge Walker's earlier ruling on this privilege. *Id. & id.* at 34-35. Thus, Judge Walker's ruling implicitly supports our opinion that the requested report is illegal insofar as it requires disclosure of classified information and/or state secrets.

As you aware, our firm is representing AT&T in this MDL proceeding 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.

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.

Irrelevance of Authorized Exclusion of Classified Information. The lawfulness of the Proposal is not affected by the fact that it states that AT&T's report "*may* exclude proprietary, classified, and confidential information, including information that would reveal the Company's litigation, regulatory, or lobbying strategy" and need not "*necessarily* refer[] to any specific programs." The only instance in which the Proposal alleges that AT&T has provided information or assistance to state or federal agencies in the absence of warrants or other such legal authorizations is in its dealings with national security agencies. In any event, AT&T could not issue a report that sets forth "the Company's policy with respect to requests for warrantless access to information about AT&T's customers" without analyzing the cooperation that it has or has not provided these agencies and without at least implicitly providing information that would confirm or deny whether the allegations about AT&T's dealings with national security agencies are true – all of which the United States has represented to be classified information over which it has also asserted its state secrets privilege. Because it is impossible to provide the requested report without providing classified information in violation of federal law, the provision of this report would be illegal.

Additional restrictions on disclosure. Revelation of information regarding the "Terrorist Surveillance Program" would be subject to further statutory prohibitions on disclosure given that the President has acknowledged that any further activity regarding this Program is conducted pursuant to the oversight of the Foreign Intelligence Surveillance Court established by the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 et seq. FISA contains an additional express section, 50 U.S.C. § 1802(a)(4), which 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 may constitute a conventional "warrant" issued upon probable cause within the vague 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 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).

More generally, under applicable provisions of the Stored Communications Act, the Director of the FBI is also 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 a report on 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 AT&T to violate one or more federal laws to which it is subject.[12]

Very truly yours,

Sidley Austin LLP

Sidley Austin LLP

DWC:dsp

[12] 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.

ADRIAN DOMINICAN SISTERS
1257 East Siena Heights Drive
Adrian, Michigan 49221-1793
517-266-3522 Phone
517-266-3524 Fax
ASinagra@adriandominicans.org
Portfolio Advisory Board

VIA FAX: 210/351-3467

November 15, 2007

Legal Department
San Antonio, TX

NOV 8 1 2007

RECEIVED

Mr. Wayne Wirtz
Assistant General Counsel
AT&T Inc.
175 E. Houston Street
P.O. Box 2933
San Antonio TX 78299-2933

The Adrian Dominican Sisters are the beneficial owners of 54,464 shares of common stock in AT&T, INC. Letters of stock verification are enclosed. Ownership of our shares will continue through the dated of the company's next annual meeting. As a representative of the Adrian Dominican Sisters, I am authorized to notify you of our intention to submit the enclosed resolution entitled: *Privacy Rights Report,* for consideration and action by shareholders at AT&T, INC's next annual meeting. We are co-sponsors with As You Sow, the primary sponsor. Other members of the interfaith Center on Corporate Responsibility may also submit filings of the enclosed resolution.

As a representative of the Adrian Dominican Sisters, I am authorized to notify you of our intention to submit the enclosed resolution entitled: *Privacy Rights Protection Report,* for consideration and action by shareholders at AT&T's next annual meeting. We will hold our shares in the company until after this meeting. We are co-sponsors of this resolution in conjunction with As You Sow, the primary filer. Other member of the Interfaith Center on Corporate Responsibility may co-sponsor this resolution as well. Therefore, I submit it for inclusion in the proxy statement in accordance with rule 14a-8 of the general rules and regulations of the security Act of 1934. We request that the Adrian Dominican Sisters be named as co-sponsors of this resolution when the company prepares its proxy materials for the next annual meeting.

Since I am faxing this filing, our institution would appreciate your sending an e-mail confirmation that all the documentation was received. My e-mail address is included below for your convenience. We are available for future dialogue as the season progresses regarding the content of the resolution.

Sincerely,

Sister Annette M. Sinagra, OP

Sister Annette M. Sinagra, OP
Corporate Responsibility Analyst
asinagra@adriandominicans.org

cc:
Mr. Edward E. Whitacre Jr.
Chairman & CEO
AT&T Inc.

EXHIBIT 1

AT&T INC.-2007
PRIVACY RIGHTS PROTECTION REPORT

RESOLVED: The shareholders of AT&T (the "Company") hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. The report should be prepared at reasonable cost and made available to shareholders within six months of the annual meeting, and it may exclude proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy.

SUPPORTING STATEMENT

The right to privacy is a long-established value, embedded in the Constitution and decades of U.S. jurisprudence, and cherished by people of all political persuasions. Privacy protections serve many important societal purposes: encouraging development of science and knowledge; preventing fraud; and allowing individuals to communicate sensitive personal information (e.g., to health care providers and clergy).

AT&T states that it is committed to the highest standards of ethics, integrity, and personal and corporate responsibility. We believe these high standards make it incumbent on AT&T to not undermine privacy rights, but rather to conduct itself in support of this American tradition of liberty which is at the foundation of our nation, democracy and basic human rights.

AT&T's reputation and good standing can be adversely affected by the perception that the Company is not adequately protecting the privacy of its customers. In our view, this threat is particularly acute in the wake of reports that AT&T voluntarily, and without a warrant, provided customer phone records and communications data to the National Security Agency.

Since reports of this cooperation first surfaced over a year ago, there have been numerous media stories, as well as public debate, on the topic. We believe that disclosure of sensitive records without a warrant is viewed by millions of Americans as, if not unlawful, then at least a violation of a customer's expectations of having telephone and e-mail records kept confidential. Telecommunications customers have choices in the marketplace and can take their business to other firms if they believe that the Company is insufficiently sensitive to these issues.

We therefore believe that AT&T should, without necessarily referring to any specific program, report to shareholders as to the Company's policy with respect to requests for warrantless access to information about AT&T customers. In our view, being able to provide a clear statement on this subject in an era of rapidly evolving technology, presents an opportunity for AT&T to play a leadership role in the protection of customer privacy rights, for the benefit of shareholders.

We urge you to vote FOR this resolution in support of privacy rights protection.

Calvert
INVESTMENTS
THAT MAKE A DIFFERENCE®

November 20, 2007

Senior Vice President and Secretary
AT&T, Inc.
175 E. Houston
San Antonio, Texas 78205

Dear Sir or Madam,

Calvert Asset Management Company, Inc. ("Calvert"), a registered investment advisor, provides investment advice for the 41 mutual fund portfolios sponsored by Calvert Group, Ltd., including Calvert's 21 socially responsible mutual funds. Calvert currently has over $16 billion in assets under management. Four of our mutual funds (the "Funds") own shares of AT&T, Inc. (the "Company").

Calvert Social Index Fund held 70,459 shares of common stock, the Calvert Social Investment Fund, Balanced Portfolio held 260,165 shares of common stock, the Calvert Variable Series, Inc., Calvert Social Balanced Portfolio held 211,277 shares of common stock, and the Calvert Social Investment Fund, Enhanced Equity Portfolio held 80,842 shares of common stock as of the close of business on November 15, 2007.

Each Fund is the beneficial owner of at least $2,000 in market value of securities entitled to be voted at the next shareholder meeting (supporting documentation enclosed). Furthermore the Funds have held 62,176, 244,965, 198,577, and 61,838 shares respectively of these securities continuously for at least one year. It is Calvert's intention that each Fund continue to own shares in the Company through the date of the 2008 annual meeting of shareholders.

I am notifying you in a timely manner that Calvert, on behalf of the Funds, is presenting the enclosed shareholder proposal for vote at the upcoming stockholders meeting. We submit it for inclusion in the proxy statement in accordance with Rule 14a-8 under the Securities Exchange Act of 1934 (17 C.F.R. § 240.14a-8).

As a long-standing shareholder, we are filing the enclosed resolution requesting that the Board of Directors prepare a report discussing privacy rights of company customers.

If prior to the annual meeting you agree to the request outlined in the resolution, we believe that this resolution would be unnecessary. Please direct any correspondence to Aditi Vora, Social Research Analyst, at (301) 961-4715, or contact her via email at Aditi.vora@calvert.com.

4550 Montgomery Avenue
Bethesda, MD 20814
800.368.2750
www.calvert.com
a UNIFI company

We appreciate your attention to this matter and look forward to working with you.

Sincerely,

William M. Tartikoff, Esq.
Vice President and Secretary

Enclosures:
Resolution Text
State Street Letter

cc: Bennett Freeman, Senior Vice President, Social Research and Policy, Calvert Group, Ltd.
Stu Dalheim, Manager of Advocacy and Policy, Calvert Group, Ltd.
Aditi Vora, Social Research Analyst, Calvert Group, Ltd.

PRIVACY RIGHTS PROTECTION REPORT

RESOLVED: The shareholders of AT&T (the "Company") hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. The report should be prepared at reasonable cost and made available to shareholders within six months of the annual meeting, and it may exclude proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy.

SUPPORTING STATEMENT

The right to privacy is a long-established value, embedded in the Constitution and decades of U.S. jurisprudence, and cherished by people of all political persuasions. Privacy protections serve many important societal purposes: encouraging development of science and knowledge; preventing fraud; and allowing individuals to communicate sensitive personal information (e.g., to health care providers and clergy).

AT&T states that it is committed to the highest standards of ethics, integrity, and personal and corporate responsibility. We believe these high standards make it incumbent on AT&T to not undermine privacy rights, but rather to conduct itself in support of this American tradition of liberty which is at the foundation of our nation, democracy and basic human rights.

AT&T's reputation and good standing can be adversely affected by the perception that the Company is not adequately protecting the privacy of its customers. In our view, this threat is particularly acute in the wake of reports that AT&T voluntarily, and without a warrant, provided customer phone records and communications data to the National Security Agency.

Since reports of this cooperation first surfaced over a year ago, there have been numerous media stories, as well as public debate, on the topic. We believe that disclosure of sensitive records without a warrant is viewed by millions of Americans as, if not unlawful, then at least a violation of a customer's expectations of having telephone and e-mail records kept confidential. Telecommunications customers have choices in the marketplace and can take their business to other firms if they believe that the Company is insufficiently sensitive to these issues.

We therefore believe that AT&T should, without necessarily referring to any specific program, report to shareholders as to the Company's policy with respect to requests for warrantless access to information about AT&T customers. In our view, being able to provide a clear statement on this subject in an era of rapidly evolving technology, presents an opportunity for AT&T to play a leadership role in the protection of customer privacy rights, for the benefit of shareholders.

We urge you to vote FOR this resolution in support of privacy rights protection.

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

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

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

EXHIBIT 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

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, Plaintiffs, v. AT&T INC., AT&T CORP., and ILLINOIS BELL TELEPHONE CO. d/b/a AT&T ILLINOIS, Defendants.	Case No. 06 C 2837 Hon. Matthew F. Kennelly

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

EXHIBIT 3

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 miliary 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 D. NEGROPONTE
Director of National Intelligence

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

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).

EXHIBIT 4

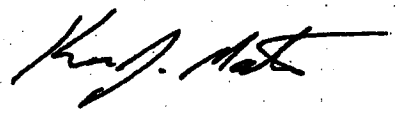
The government has moved to dismiss the action on the basis of the military and state secrets privilege. *See Hepting*, Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America (May 12, 2006). Its motion is accompanied by declarations from John D. Negroponte, Director 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.

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

Sincerely,



Kevin J. Martin
Chairman

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

EXHIBIT 5

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

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

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

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

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

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

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

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

---

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

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

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

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

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

---

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

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

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

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

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

* * *

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

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

Sincerely,

Peter D. Keisler

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

Attachments

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PEOPLE FOR THE AMERICAN WAY FOUNDATION	)	
Plaintiff,	)	
v.	)	**Civil Action No. 06-206 (ESH)**
NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE,	)	
Defendant.	)	

MEMORANDUM OPINION

Plaintiff People for the American Way Foundation has sued the National Security Agency ("NSA") under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, seeking documents relating to the NSA's recently revealed Terrorist Surveillance Program ("TSP"). The issue before the Court is whether the NSA properly invoked various statutory exemptions under FOIA to withhold documents responsive to plaintiff's requests, and to refuse to confirm or deny the existence of other responsive documents. Plaintiff has withdrawn a number of its original requests, and defendant has moved for summary judgment with respect to all of plaintiff's remaining FOIA requests. Plaintiff has also moved for summary judgment with respect to three of its requests, and has opposed defendant's motion for summary judgment on the other two remaining requests. As explained herein, the Court grants defendant's motion for summary judgment and denies plaintiff's motion.

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.[3/]

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

---

[3/]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.[5/] *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

---

[5/]In 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),[6/] 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),[7/] 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

---

[6/]This 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).

[7/]*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.[8] *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

---

[8]Because 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").

ACLU, 265 F. Supp. 2d at 30.

CONCLUSION

For the foregoing reasons, the Court holds that the NSA properly invoked Exemptions 1 and 3 to withhold information responsive to plaintiff's FOIA requests 2-4 and 6 and to refuse to confirm or deny the existence of documents responsive to request 16. Thus, defendant "has fully discharged its obligations under the FOIA." *Greenberg*, 10 F. Supp. 2d at 11. Defendant's motion for summary judgment is therefore granted, and plaintiff's motion for partial summary judgment is denied.

/s/
ELLEN SEGAL HUVELLE
United States District Judge

Date: November 20, 2006

Appendix
8

at&t

opyright and Privacy Policy

AT&T Privacy Notice

Effective 06/16/06

OUR COMMITMENT: RESPECTING AND PROTECTING YOUR PRIVACY

THE SCOPE OF THIS PRIVACY POLICY

WHAT PERSONAL IDENTIFYING INFORMATION WE COLLECT, HOW WE USE IT AND HOW YOU CAN CONTROL ITS USE

- **Personal identifying information we collect and use**
- **Personal identifying information we disclose to third parties**
- **Information included in our directories and directory assistance service**
- **Obtaining non-published and non-listed numbers**
- **Our "Do Not Call" lists**
- **Customer Proprietary Network Information**

WHAT ONLINE INFORMATION WE COLLECT, HOW WE USE IT AND HOW YOU CAN CONTROL ITS USE

- **Web usage information we collect and use**
- **How we use cookies, Web beacons, etc.**
- **Our e-mail marketing practices**
- **Our policy on online access by children**
- **Linking to other sites**
- **Online privacy education**

HOW WE PROTECT YOUR INFORMATION

PRIVACY POLICY UPDATES

CONTACTING US: QUESTIONS, COMMENTS, CONCERNS

Back to Privacy Summary

OUR COMMITMENT: RESPECTING AND PROTECTING YOUR PRIVACY

The AT&T family of companies ("AT&T") recognizes that the trust of our customers and Web visitors requires vigilant, responsible privacy protections.

We respect and protect the privacy of our customers. As a provider of telecommunications and related services and products we recognize that we must maintain the confidentiality of every customer's telephone calling and other account information.

We also respect and protect the privacy of our Web visitors. The expansion of online services and changing technologies continues to create unique privacy concerns and we recognize the need to maintain the confidentiality of information that Web visitors reasonably expect to remain private.

We have a long history of vigorously protecting customer and web visitor privacy. Our customers and web visitors expect, deserve and receive nothing less than our fullest commitment to their privacy. We also have an obligation 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. If and when we are asked to help, we do so strictly within the law and under the most stringent conditions.

* AT&T Inc. was created on Nov. 18, 2005, through a merger of SBC

Communications Inc. and AT&T Corp. We continue to undergo branding changes to bring together all former SBC and AT&T brands and this privacy policy applies irrespective of AT&T or SBC branding.

top

THE SCOPE OF THIS PRIVACY POLICY

- This privacy policy addresses the privacy of AT&T retail customers and Web visitors in the United States. Where applicable, AT&T will comply with the laws of other countries that contain mandatory requirements that differ from this policy. In selected jurisdictions outside the United States, a member of the AT&T family of companies may adopt a separate privacy policy to reflect the requirements of applicable local laws.
- This policy identifies the types of data and information we collect, how we use it, how you can control its use and the steps we take to protect it. The primary focus of this policy is non-public information that identifies or that is linked to the identity of a customer or Web visitor ("personal identifying information").
- In this policy, the AT&T family of companies means AT&T Inc. and its subsidiary and affiliated entities. Members of the AT&T family of companies have agreed to the privacy practices in this policy - except for Cingular® Wireless and YELLOWPAGES.COM, both of which are joint ventures between AT&T and Bell South and operate under their own privacy policies. Personal identifying information shared between Cingular® Wireless or YELLOWPAGES.com and other AT&T family of company members will be used and protected as set forth in this policy.
- This policy does not apply where non-members of the AT&T family of companies ("third parties") have licensed the AT&T brand for use with their own products or services. For example, the policy does not apply to Advanced American Telephones, which licenses the AT&T Brand to sell telephone equipment, or to Citibank, which licenses the AT&T Brand to offer its AT&T Universal Card.
- When you sign up for certain AT&T-offered services, you may agree to additional privacy policies that address service-specific privacy practices. For example, certain AT&T Internet services - AT&T Yahoo! Dial, AT&T Yahoo! DSL, AT&T Yahoo! Small Business and AT&T Yahoo! Geocities - and AT&T U-verse TV and Homezone services are subject to an additional privacy policy. View a copy of the AT&T Yahoo! and Video Services policy. Similarly, AT&T | DISH network service is subject to an additional privacy policy.

top

WHAT PERSONAL IDENTIFYING INFORMATION WE COLLECT, HOW WE USE IT AND HOW YOU CAN CONTROL ITS USE

Personal identifying information we collect and use

- We collect personal identifying information regarding our customers, including information customers give us, information collected as a result of the customer's relationship with us and information we obtain from other sources. Examples include name; address; e-mail address; telephone number; billing, payment, usage, credit and transaction information (including credit card numbers, account numbers and/or social security number); and demographic information.
- We also collect personal identifying information that our Web visitors choose to provide to us (e.g., name, address, telephone number, e-mail address) when registering on our Web sites; ordering AT&T-offered products or services; sending us e-mail; responding to our surveys; entering contests or sweepstakes; or in connection with online ordering or billing functions.
- We use the personal identifying information of a customer to provide, confirm, change, bill, monitor and resolve problems with the quality of AT&T-offered products and services. We also use the personal identifying information of a customer or Web visitor to develop, market and sell our products and services.
- We may aggregate the personal identifying information of different customers or Web visitors to produce data about a group or category of services, customers or Web visitors. For example, we might use aggregate data about the types of services our customers have generally purchased at the same time in order to develop attractive bundled service offerings. Such aggregate data, however, will not reflect any personal identifying information of any specific customer or Web visitor.

Personal identifying information we disclose to third parties

- We do not provide personal identifying information (other than information included in our directories and directory assistance service) to third parties for the marketing of their products and services without your consent.
- We may provide personal identifying information to third parties where required to provide certain AT&T-offered products and services. For example, we disclose

certain AT&T | DISH Network-related personal identifying information to Echostar Satellite Corporation, L.L.C. and its affiliates solely in order to provide AT&T | DISH Network services.

- We may also provide personal identifying information to third parties who perform functions or services on our behalf. Examples include shipping companies who deliver AT&T products; AT&T-authorized agents who market and sell AT&T-offered products and services on our behalf; and Web site development or advertising companies, who provide Web design, analysis and advertising services.
- When we provide such personal identifying information to third parties to perform such functions or services on our behalf, we require that they protect personal identifying information consistent with this policy and do not allow them to use such information for other purposes.
- We may, where permitted or required by law, provide personal identifying information to third parties (including credit bureaus or collection agencies) without your consent:
  - To obtain payment for AT&T-offered products and services, enforce or apply our customer agreements, and/or protect our rights or property.
  - To comply with court orders, subpoenas, or other legal or regulatory requirements.
  - To prevent unlawful use of communications or other services, to assist in repairing network outages, and when a call is made to 911 from a customer phone and information regarding the caller's location is transmitted to a public safety agency .
  - To notify a responsible governmental entity if we reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without delay.
- A customer's name and telephone number may also be transmitted and displayed on a Caller ID device unless the customer has elected to block such information. Caller ID Blocking does not prevent the display of the number when you dial certain business numbers, 911, 900 numbers or toll-free 800, 888, 877 or 866 numbers.

Information included in our directories and directory assistance service

- We publish and distribute directories in print, on the Internet, and on CDs and/or other electronic media (some complimentary and some for a fee). These directories include limited personal identifying information about our customers - i.e., published customer names, addresses and telephone numbers - without restriction to their use. Our directories may also include information obtained from third parties. We also make that information available through directory assistance operators and through the Internet. For more information on controlling the disclosure of this information, see Obtaining non-published and non-listed numbers below.
- We are required by law to provide published customer names, addresses and telephone numbers (or non-published status) to unaffiliated directory publishers and directory assistance providers, over whom AT&T has no control, for their use in creating directories and offering directory assistance services.
- This directory information is not legally protected by copyrights and may be sorted, packaged, repackaged and made available again in different formats by anyone, including AT&T.

Obtaining non-published and non-listed numbers

- Except as described below, telephone listings of AT&T local telephone customers are made available in our directories and through directory assistance.
- When a customer subscribes to AT&T local telephone service, we offer the opportunity to request that the customer's name, number, and address not be published in our directories or made available through our directory assistance.
  - The names, numbers and addresses of customers who choose to have a "non-published" number will not be available in our directories or through our directory assistance. Likewise, we do not make non-published numbers available to others to include in directories or to provide directory assistance services.
  - The names, numbers and addresses of customers who choose to have a "non-listed" number will not be available in AT&T directories, but the information will be publicly available through directory assistance and will be provided to unaffiliated directory assistance providers over whom AT&T exercises no control.
  - There is a fee for customers who choose to have non-published or non-listed telephone numbers.
  - Customers may choose to exclude partial or all address information from their listings.
  - Customers in Nevada do not have the option of a non-listed number.

For more information, contact an AT&T service representative.

Our "Do Not Call" lists

- We comply with all applicable laws and regulations regarding "Do Not Call" lists. These laws generally permit companies to contact their own customers even though such customers are listed on the federal and, in some instances, state "Do Not Call" lists.
- Residential consumers may request that they be removed from AT&T's telemarketing lists at any time, including when an AT&T marketing and promotional call is received or by contacting an AT&T service representative.
- Where required by state laws and/or regulations, we also honor requests from business customers to be removed from our telemarketing lists.
- Cingular® Wireless maintains its own "Do Not Call" policy and lists. Please contact Cingular Wireless directly at 1-866-CINGULAR if you wish to be placed on its "Do Not Call" list.

Customer Proprietary Network Information

- In the normal course of providing telecommunications services to our customers, we collect and maintain certain customer proprietary network information, also known as "CPNI". Your CPNI includes the types of telecommunications services you currently purchase, how you use them and related billing information for those services. Your telephone number, name and address are not CPNI.
- Protecting the confidentiality of your CPNI is your right and our duty under federal law. We do not sell, trade or share your CPNI - including your calling records - with anyone outside of the AT&T family of companies or with anyone not authorized to represent us to offer our products or services, or to perform functions on our behalf except as may be required by law or authorized by you.
- As a general rule, we are permitted to use CPNI in our provision of telecommunications services you purchase, including billing and collections for those services. We are permitted to use or disclose CPNI to offer telecommunications services of the same type that you already purchase from us. We may also use or disclose your CPNI for legal or regulatory reasons such as a court order, to investigate fraud or to protect against the unlawful use of our telecommunications network and services and to protect other users.
- Click here for more information on the use of CPNI.

top

WHAT ONLINE INFORMATION WE COLLECT, HOW WE USE IT AND HOW YOU CAN CONTROL ITS USE

Web usage information we collect and use

- When Web visitors access our Web sites we automatically receive certain "Web usage" information. For example, our Web servers automatically collect the visitor's IP address, the visitor's Web browser and operating system types, and the identity of the Web page from which the visitor's browser entered our Web site. In addition, primarily through the use of cookies or Web beacons, we may collect other Web usage information, such as the Web pages the browser visits on our Web sites, the amount of time spent on such Web pages and whether the browser re-visits our Web sites/pages.
- We use Web usage information to facilitate and enable the functioning of our Web sites and to expand and improve our Web visitors' online experience. We may also aggregate such Web usage information with other visitors' Web usage information to assess trends and better design, monitor and otherwise improve our Web sites, as well as to focus our marketing efforts.
- In some cases we may combine Web usage information related to your access to our Web sites with personal identifying information. We use the combined information to provide our customers and Web visitors with a better online experience by providing customized features and services and to market and provide advertising about goods and services that may be of particular interest. Once combined, the resulting data is protected as personal identifying information as described in this policy.

How we use cookies, Web beacons, etc.

- Cookies are alphanumeric identifiers that a Web server sends to your computer when you visit a Web site. Cookies can contain a variety of information, such as a simple count of how often you visit a Web site or information that allows us to customize our Web site for your use. Web beacons (also known as "clear gifs" or "one-pixel gifs") are small graphic images on a Web page or in an e-mail that allow us to monitor the activity on our Web sites or to make cookies more effective.
- We, or a third party acting on our behalf, may use "cookies" to tailor and improve the content we deliver to our Web visitors, to improve our Web sites by assessing which areas, features, and products are most popular, and to personalize our Web sites and make recommendations based on information, including product choices, a particular visitor has previously provided. For example, we may use a

cookie to identify your state so we do not ask you to enter it more than once. We also use cookies to store user preferences, complete online order activity and keep track of transactions.

We, or a third party acting on our behalf, may use Web beacons in certain of our Web pages and e-mails to gauge the effectiveness of our marketing campaigns and e-mail correspondence. For example, we may use Web beacons in our HTML-based e-mails to let us know which e-mails have been opened by the recipients.

You can configure your Web browser to alert you when a Web site is attempting to send a cookie to your computer and allow you to accept or refuse the cookie. You can also set your browser to disable the capacity to receive cookies or you can delete cookies previously accepted. Some AT&T Web pages (and other Web pages) may not work correctly if you have cookies disabled.

We may use advertising companies to deliver ads for AT&T-offered services and products on our Web sites or on third party Web sites. These Internet ads are often called "banner ads" and may contain third-party cookies or Web beacons that allow tracking of visitors' responses to our advertisements. Although these third parties may receive anonymous Web usage information about ad viewing on such Web sites, we prohibit them from using this information for any purpose other than to assist us in measuring the effectiveness of our ads.

We may also accept third party advertisements on our Web sites. You should refer to the privacy policy of these advertisers for information regarding their use of cookies and collection of information. You can visit the Network Advertising Initiative Web site to opt out of certain network advertisers' cookies.

Our e-mail marketing practices

We periodically send customers news and updates via e-mail regarding AT&T-offered services, products, and special promotions. Every marketing e-mail we send contains instructions and an opt-out link that will allow you to stop additional AT&T marketing e-mails based on line of business.

We do not provide your e-mail address to third parties for the marketing of third-party products without your consent.

Our policy on online access by children

AT&T Web sites are not designed to attract children under the age of 13. We do not target children for the collection of information online and do not knowingly collect personal identifying information from anyone under the age of 18.

Ordering online products and services from AT&T is limited to adults (age 18 or over or as otherwise legally defined).

We comply with all applicable laws and regulations, including the Children's Online Privacy Protection Act (COPPA), which requires the consent of a parent or guardian for the collection of personally identifiable information from children under 13.

Linking to other sites

Our Web sites may provide links to third party sites. We are not responsible for the privacy, security or content of such sites. If you are asked to provide information on one of these Web sites, we encourage you carefully to review their privacy policy before sharing your information.

Online privacy education

We care about the privacy of our customers and Web visitors and strive to provide you with relevant information to help you learn how better to protect your privacy and security while online. Please visit the AT&T Internet Safety Web site and the AT&T Worldnet Security Center.

top

HOW WE PROTECT YOUR INFORMATION

All AT&T employees are subject to the AT&T Code of Business Conduct and certain state-mandated codes of conduct. The AT&T Code requires all our employees to follow every law, rule, regulation, court and/or commission order that applies to our business at all times. In addition, the Code specifically requires compliance with legal requirements and company policies related to the privacy of communications and the security and privacy of customer records. Employees who fail to meet any of the standards embodied in the Code of Business Conduct may be subject to disciplinary action, up to and including dismissal.

We employ security measures designed to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data, including personal identifying information. We have implemented technology and security features

and strict policy guidelines to safeguard the privacy of your personal identifying information, and we will continue to enhance our security procedures as new technology becomes available. For example:

- We maintain and protect the security of our servers and we typically require user names and passwords to access sensitive data.
- We use industry standard encryption methods to protect your data transmission unless you authorize unencrypted transmission.
- We limit access to personal identifying information to those employees, contractors, and agents who need access to such information to operate, develop, or improve our services and products.

If we determine that a security breach has occurred and that such breach creates a risk of identity theft or service disruption, we will make reasonable attempts to notify you.

top

PRIVACY POLICY UPDATES

- This privacy policy supersedes and replaces all previously posted privacy policies.
- We want you to be aware of the information we collect, how we use it and under what circumstances, if any, we disclose it. We reserve the right to update this privacy policy to reflect any changes we make in order to continue to serve the best interests of our customers and Web visitors and will timely post those changes. If we make a material change to this privacy policy, we will post a prominent notice on our Web sites.
- If we intend, however, to use personal identifying information in a manner materially different from that stated at the time of collection, we will attempt to notify you at least 30 days in advance using an address or e-mail address, if you have provided one, and by posting a prominent notice on our Web sites, and you will be given a choice as to whether or not we use your information in this different manner.
- Please periodically check our Web sites for changes to this privacy policy.

top

CONTACTING US: QUESTIONS, COMMENTS, CONCERNS

- AT&T honors requests from customers and Web visitors to review their personal identifying information that we maintain in reasonably retrievable form and we will gladly correct any such information that is inaccurate. You may verify that appropriate corrections have been made. Please contact an AT&T service representative.
- If you are receiving unwanted e-mails at or from an SBC Yahoo! e-mail address (e.g., @sbcglobal.net, @yahoo.com) please visit the AT&T Yahoo! Anti-Spam Resource Center. For AT&T Worldnet unwanted e-mails, please visit the AT&T Worldnet Spam Center.
- We are happy to address any concerns you may have about our privacy practices and policies. You may e-mail us at privacypolicy@ATT.com or write to us at AT&T Privacy Policy, 175 E. Houston St., San Antonio, TX 78205.
- AT&T is a TRUSTe licensee. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. Because AT&T wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe. The TRUSTe program covers only information collected through AT&T Web sites, and does not cover information that may be collected through software downloaded from such sites.
- AT&T's privacy policy and practices also meet the requirements of the Better Business Bureau's Online Privacy Program, and we proudly display the BBBOnLine Privacy Seal. Further information about this program is available at http://www.bbbonLine.org.
- If you have questions or concerns regarding this policy, you should first contact us via e-mail at privacypolicy@att.com. If you do not receive acknowledgment of your inquiry or your inquiry is not satisfactorily addressed, you should then contact TRUSTe through the TRUSTe Watchdog Dispute Resolution Process and TRUSTe will serve as a liaison to resolve your concerns. You may also contact BBBOnLine at http://www.bbbonLine.org.

top

Jonas D. Kron, Attorney at Law

2940 SE Woodward Street
Portland, Oregon 97202
(971) 222-3366 ~ (801) 642-9522
jdkron@kronlaw.com

January 7, 2008

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 2008 Proxy Statement

Dear Sir/Madam:

I have been asked by Calvert Asset Management Company, Inc., Larry Fahn, and The Adrian Dominican Sisters (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 "the 2008 Proposal" or "the Proposal") to AT&T, to respond to the letter dated December 18, 2007 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 2008 proxy statement by virtue of Rules 14a-8(b), 14a-8(f), 14a-8(i)(2), 14a-8(i)(3), 14a-8(i)(6), 14a-8(i)(7) and 14a-8(i)(10).

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 2008 proxy statement, because (1) the Proponents are eligible to submit the Proposal; (2) the Proposal, if implemented, would not cause the Company to violate the law; (3) the subject matter of the Proposal transcends the ordinary business of the Company by focusing on a significant social policy issue, (4) the Proposal will have no substantive affect on any pending or contemplated litigation, (5) contrary to the Company's argument, is in no way vague or indefinite, and (6) the requested report is not moot. Therefore, we 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. Legal Department Senior Attorney Paul Wilson.

Summary Response

After the rigorous review of a similar proposal last year, the Proponents have taken this opportunity to redraft the Proposal with the conclusion of the Staff in mind. The Proposal we have submitted falls well within the parameters of Rule 14a-8 and represents the legitimate concerns of long standing AT&T shareholders which we rightfully seek to place on the Company proxy materials. The Proposal

submitted by the Proponents is in direct response to the February 22, 2007 no-action letter issued by the Staff. In that letter, the Staff specifically stated that because it related to "litigation strategy" it was excludable. Having taken that decision into due consideration, the Proponents have filed a new proposal that is drafted to meet the Staff's guidance.

Virtually every aspect of the Company's no-action request is based on a misinterpretation of the Proposal. In the last analysis we urge the Staff to conclude that the Proposal simply focuses on the significant social policy issues raised by allegations that the Company disclosed customer records and content of customer communications to the government without a warrant. The Company has tried to create the impression that the subject matter of the Proposal is the detailed language of its privacy policies and past practices. We are interested in seeing management engage in a discussion of the social policy issues of privacy rights at stake from technological, legal and ethical standpoints. We are not interested in delving into the minutiae of the Company's privacy procedures or website published company policies. The Proposal does not ask for a specific result, policy or disclosure of litigated information, but an exploration of the issues as they apply to the Company's future as a profitable and responsible company. As the SEC and the courts have made clear, shareholders have the right to raise significant social policy issues with companies. As discussed more fully below, there is no doubt that the Company's conduct with respect to the disclosing customer information and communications is a significant social policy issue it needs to address. This Proposal is specifically focused on this policy issue the Company is facing and properly requests a report that discusses it.

Finally, the July 2006 order of Judge Vaughn R. Walker, of the U.S. District Court for the Northern District of California, in *Hepting v. AT&T* makes it clear 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 (TSP) 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. 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: The shareholders of AT&T (the "Company") hereby request that the Board of Directors prepare a report that discusses from technical, legal and ethical standpoints, the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. The report should be prepared at reasonable cost and made available to shareholders within six months of the annual meeting, and it may exclude proprietary, classified and confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy.

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, a group of shareholders including the Proponents filed a shareholder resolution with the Company in October 2006 (hereinafter "the 2007 Proposal"). That proposal read 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.

In February 2007, the Staff excluded the 2007 Proposal as relating to the Company's ordinary business ("litigation strategy"). As is evident, the 2008 Proposal is significantly different from the 2007 Proposal. Nevertheless, both proposals had the same fundamental goal - to focus the attention of management on the social policy issue of privacy rights in the context of disclosing customer information without a warrant and the long-term wellbeing of the Company.

The goal of the 2008 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 rights in the context of disclosing customer information without a warrant. 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, law enforcement or its litigation position. Rather it seeks a report from the Company that can serve as basis for discussions about the role the Company will take, in social policy terms, in its pivotal position of control over customer communication data and content.

ANALYSIS

I. The Proponents are Eligible to Submit the Proposal.

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

III. 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 that Transcends the Day-to-day Affairs of the Company..

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 privacy rights.

3. Legal Compliance:the Proposal is not focused on legal compliance, but rather on social policy issues.

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

---

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." A*malgamated 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).

5. "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.

IV. AT&T's privacy policies for customers are not substantial implementation of the Proposal because the Proposal seeks a discussion of privacy rights issues with shareholders.

I. The Proponents are Eligible to Submit the Proposal.

The Company's first claim is astonishing in its attempt over five pages of excessive parsing and verbal smoke and mirrors, plus 32 pages of appendices to bury a simple fact: there is no question that the Proponents have owned the requisite number of shares well in excess of the one year requirement. The purpose of Rules 14a-8(b) and 14a-8(f) is to ensure that the proponents "have some measured economic stake or investment interest in the corporation." Exchange Act Release No. 34-20091 (August 16, 1983). The purpose is to curtail abuse of the shareholder proposal rules, *id.*, not to provide an opportunity for corporations to abuse the rule by raising spurious arguments and covering the proponents in paper in an effort to derail the process.

Proponent Calvert's ownership eligibility is virtually self-evident. On November 20, 2007 Calvert's letter of submission stated that it held well in excess of 500,000 shares of AT&T continuously for at least one year. It also stated that it is Calvert's intention to own those shares of the Company through the 2008 Annual Meeting. On November 26, 2007 AT&T sent its documentation request letter to Calvert stating "On November 21, 2007, we received your letter dated November 20, 2007, submitting a stockholder proposal" and requesting documentary support. (Company's Appendix 5). The Company did not identify any documentary deficiencies in that letter. Calvert promptly responded on December 6, 2007 clearly stating "**that each of these funds has continuously held these shares for at least one year prior to the date we submitted the proposal**" - November 20, 2007. This letter was accompanied by a December 3, 2007 letter from State Street documenting continuous ownership through the November 20th submission date and December 3, 2007. (Company's Appendix 6).

The Company has tried to manufacture ambiguity from the fact that State Street's letter used two columns – total holdings for each Calvert fund and then holdings in each fund for more than a year - suggesting that it is not clear which date the holdings refer to. Despite this verbose attempt, the December 3rd State Street letter and the clear language of Calvert's December 6, 2007 letter make it evident that Calvert has owned the requisite shares for a continuous period of time in excess of one year prior to submission. Calvert has also made it clear that it will continue to hold those shares through the Annual Meeting. Accordingly, we urge the Staff to reject the Company's argument.

To the extent the Company's argument is that the submission date was November 21st rather than November 20th, in addition to the preceding paragraph we would point out that the Company's November 26th letter clearly leaves one with the impression that it considered November 20th to be the submission date. For all of the above reasons, the Company's argument fails under Rule 14a-8(b), 14a-8(f) and Staff Legal Bulletin No. 14 (July 13, 2001). Under these standards, the Company must "provide adequate detail about what the shareholder must do to remedy all eligibility or procedural

defects." This advice was reaffirmed in Staff Legal Bulletin 14B (September 15, 2004), Section C.1. The Company's letter failed to indicate clearly its position on this point and did not take any steps to clarify that point when the Calvert asserted November 20th as the submission date. The Company cannot switch the dates around in this manner and we respectfully request the Staff reject this line of argument.

With respect to Proponent Adrian Dominican Sisters (hereinafter "ADS"), the Company clearly concedes that ADS purchased the requisite amount of AT&T stock more than one year before the proposal was submitted. It is also clear from a common sense reading of ADS's reply to the Company's deficiency letter that ADS continued to own the shares at that time and would continue to do so through the Annual Meeting. The Company appears to be using this opportunity to sow seeds of confusion and in the process create the appearance of a technical error on the part of ADS. To allow this kind of argument to prevail would elevate form over substance and turn the informal no-action letter process that is intended to be simple to administer into a technical obstacle course. As the SEC explained in Exchange Act Release No. 34-20091 (August 16, 1983) when justifying its adoption of the plain-English format, the goal is to "make the rule easier for shareholders and companies to understand and follow." This kind of argument from the Company does not serve those purposes. Clearly, ADS has, in the words of the SEC, an "economic stake or investment interest in the corporation." As such, we request the Staff to conclude ADS is eligible to file the Proposal.

Finally, the Company has failed to acknowledge Larry Fahn as a co-filer of the Proposal. Attached as Appendix A is Mr. Fahn's cover letter and a copy of the Proposal. Also attached is documentation from UPS's tracking service showing that Mr. Fahn's filing was received at the Company's executive offices in San Antonio, Texas on the afternoon of November 21, 2007. This documentation proves that Mr. Fahn co-filed the proposal with ADS and Calvert in advance of the November 23, 2007 deadline. Consequently, Mr. Fahn has met the requirements of the Rule and is a co-filer of the Proposal. Despite AT&T's timely receipt of Mr. Fahn's submission, and despite the fact that his co-sponsorship was mentioned in the letters from Calvert (Company's Appendix 7) and ADS (Company's Appendix 3), the Company inexplicably chose to act as if it never received this correspondence. Nor did the Company comply with Rule 14a-8(b) and (f), which requires timely notice to a proponent if the company believes that timely filed documentation is insufficient. The time for AT&T to raise any technical objections as to Mr. Fahn's eligibility has long since passed, and thus we respectfully request that the Staff advise the Company of its view that Mr. Fahn should be viewed as a co-filer.

II. 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 conclude that the Company has not met its burden of persuasion and the Proposal is permissible under Rule 14a-8(i)(2).

Before providing an analysis of the Rule in this circumstance, there are two features of the Company

and Sidley letters that are quite remarkable. First, there is no discussion whatsoever about Rule 14a-8(i)(2). While there is a discussion of various federal national security laws, there is no discussion of the proxy rules or how the national security laws interact with the Rule. Under *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 SEC no-action letter. Nor has it even gone beyond a mere recitation of Rule 14a-8(i)(2), let alone discuss any examples 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 even tried to cite to any decided legal authority or compelling precedent on this issue.

Second, our analysis for the 2007 Proposal included an extensive discussion of Judge Walker's July 20, 2006 Order ("Order") in *Hepting v. AT&T Corporation.* Appendix B. It would appear that the Company would prefer that this order did not exist and instead of addressing the points raised by Judge Walker and cited by the Proponents, is seeking to ignore it. Last year, the Company filed a second letter that did not provide any analysis of Judge Walker's order and this year they have not even mentioned it. We would contend that this is because Judge Walker's order is fatal to the Company's argument.

Turning to an analysis of the case, 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 case[2] and consequently, this claim by the Company does not succeed. If such a claim is to the 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 sought, it is false to argue that the Company can say no more than it can neither confirm nor deny its participation in the program. This issue was discussed at length by Judge Walker, who had been assigned to hear the consolidated lawsuits related to claims against the telecommunications companies. Specifically, 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.

---

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.

Order at p. 29 (emphasis added) Appendix B. 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, 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. See *id.* at pp. 28 – 42 for a fuller discussion of his findings.

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 pp. 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) 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.

Judge Walker's conclusions gained further support on November 16, 2007 when the Ninth Circuit handed down its decision in a companion case, *Al-Haramain Islamic Foundation, Inc. v. Bush*, No. 06-36083 (9th Cir. November 16, 2007). *Hepting* and *Al-Haramain* were argued before the Ninth Circuit in August 2007, but thus far there has only been a decision in *Al-Haramain* – the *Hepting* case remains pending. While that decision does not address precisely the same issues as does the *Hepting* case, the court does state the following:

> In light of extensive government disclosures about the TSP, the government is hard-pressed to sustain its claim that the very subject matter of the litigation is a state secret. Unlike a truly secret or "black box" program that remains in the shadows of public knowledge, the government has moved affirmatively to engage in public discourse about the TSP. Since President Bush's initial confirmation of the program's existence, there has been a cascade of acknowledgments and information coming from the government, as officials have openly, albeit selectively, described the contours of this program. Thus, we agree with the district court that the state secrets privilege does not bar the very subject matter of this action.

Id at pp. 14960 – 14961. As such, both the trial court and appellate court have concluded that the subject matter of warrantless surveillance is not a state secret.

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. Last year, the Company did seek to make a couple of specific arguments regarding specific language in the 2007 Proposal regarding notification of customers and expenditures. These two provisions have been removed from the Proposal and consequently the Company is left without any specific language to take issue with. Thus, the Company's primary argument appears to be 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 contrast, 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 kind of discussion about the policy issues surrounding AT&T's alleged cooperation with government agencies. Last year's 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 of last year's letter 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, the ethical questions raised and the responsible role of a corporation in weighing those social policy issues – is clear. A report could be written that discusses these social policy issues without revealing classified information.[3] 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 requests for cooperation as described in media stories, in short in can be a generalized discussion of the policy issues that the Company is facing when privacy issues in the context of disclosing customer information without a warrant are raised.

---

3 We note that the Company has cited *People for the American Way Foundation v. NSA.*, Civil Action No. 06-206 (ESH) (D.D.C. 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 14a-8); 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.

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.[4]

Also, we note that other telecommunications companies, specifically Qwest, BellSouth and Verizon, 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 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>. Appendix C.

As 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.

Order at page 41. Given that these companies apparently did 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 turning the Proposal into something it is not. For example, on page three, the Company's attorney contends that the report called for by the Proposal would require "analyses" of Company interactions with federal agencies. In this way, the Sidley letter tries to paint the Proposal as seeking highly detailed information about the Programs.

These characterizations could not be farther from the truth. The plain language of the Proposal asks for a report that discusses "*policy issues* that pertain to disclosing customer records . . ." Rule 14a-8 is designed to allow shareholders to raise "significant social policy issues" in shareholder proposals. That is precisely what the Proposal does. Disclosure of customer records and the content of customer communications raises significant social policy issues for the Company. The Proponents are simply asking the Company in the resolved clause to "discuss" those issues – not to "analyze" minutia or to declaratively set forth a company policy or procedure. While it is clear that the Proponents think it is advisable to adopt a policy that shows the Company is a leader in protecting privacy rights in the context of disclosing customer information without a warrant the Proposal does not ask the Company to do that. Rather, the Proposal seeks a discussion of the policy issues facing the Company. As the court in *Medical Committee for Human Rights Medical*, 404 U.S. 402 (1972) explained, it is our duty as shareholders to discuss the moral ramifications of the company's business. That is the goal of the Proposal.

---

4 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.

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, 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 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 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 a social policy 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.

III. 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 that Transcends the Day-to-day Affairs of the Company.

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 & Co.*, 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* (emphasis added).

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).

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. See the following attached in Appendix C:

- An October 2007 Mellman Group Poll found that "Sixty-one percent of voters favor requiring

the government to get a warrant from a court before wiretapping the conversations U.S. citizens have with people in other countries, with an outright majority of voters, 51 percent, 'strongly' supporting the requirement, the poll of 1,000 likely 2008 general-election voters found." http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/10/16/poll_us_voters_oppose_bush_wiretap_law/6209/. 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. 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. This clearly demonstrates that the issue has persistent and widespread interest in American society.

- Very recently, the issue of AT&T receiving immunity related to warrantless wiretapping has received heavy Congressional and media attention – and even entering the 2008 Presidential campaigning. See the following also contained in Appendix C:
  - ABC News. December 17, 2007. *Dodd Succeeds in Delaying Wiretapping Bill.*
  - Associated Press. December 17, 2007. *Surveillance Bill Delayed Until 2008.*
  - Baltimore Sun. December 17, 2007. *Senate punts on FISA bill in face of discord.*
  - CBS News. December 17, 2007. *FISA Debate in Senate Delayed Until January.*
  - CNNMoney.com. December 17, 2007. *Wiretapping Bill Debate Continues; No Immunity Vote.*
  - Detroit Free Press. December 18, 2007. *Security vs. privacy in Senate.*
  - The New York Times. December 18, 2007. *Democrats Delay a Vote on Immunity for Wiretaps.*
  - Reuters. December 17, 2007. *U.S. Senate postpones consideration of spy bill.*
  - San Francisco Chronicle. December 19, 2007. *Feinstein offers compromise: secret court review of wiretap cases.*
  - Washington Post. December 18, 2007. *Telecom Immunity Issue Derails Spy Law Overhaul.*

- The issue has resulted in numerous reports by print, radio, television and Internet media. Attached is a partial list of more than 40 stories on the issue from media outlets including the New York Times, the Weekly Standard, 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 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." Cox News, November 15, 2006, *Bush is seeking immunity for telecom industry*. Senator Leahy recently said "While I appreciate the problems facing the telecommunications companies, the retroactive immunity issue to me is not about fixing blame on the companies but about holding government accountable. Passing a law to whitewash the administration's undermining of another law would be a disservice to the American people and to the rule of law." CBS News. December 17, 2007. *FISA Debate in Senate Delayed Until January.*

- As the documents in Appendix C demonstrate , 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. Hearings on the issue have been held in a number of other states including Washington, Delaware, Nebraska, and Pennsylvania.

- 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.

- The possibility that AT&T has shared phone records has also exposed the company to substantial potential liability. More that 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 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 .

- Another 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/>

- At Cisco Systems, Inc.'s November 2007 Annual Meeting, 49.5% of all shareholders voted against management's recommendation and supported Boston Common's proposal with a "For" (28.5%) or "Abstain" (21%) vote on 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*** . . ." In 2006 the number of "For" or "Abstain" votes were 29%. These votes and the voting trend are a clear expression of considerable shareholder concern about the role that

technology and communications companies play in the freedom of expression and privacy. InformationWeek. November 15, 2007. Cisco Shareholders Shelve Human Rights Resolution.

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 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 Proposal and the resulting controversy and financial risks transcend the day-to-day affairs of the Company. These are issues about which shareholders are appropriately concerned, and as a result shareholders have the right to raise these issues at AT&T's annual meeting and express their opinions about how the Company should explore its role in protecting privacy rights in the context of disclosing customer information without a warrant. 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.

In response to the Staff no-action letter as to the 2007 Proposal, the Proponents redrafted the Proposal so as to assiduously avoid any implication that the Proposal relates to the Company's litigation strategy. We have removed all references to AT&T's past expenditures on attorney's fees and expert's fees. Furthermore, we have crafted a proposal that focuses on the social policy issues that pertain to customer privacy and not on "specified information". It is abundantly evident from the plain text of the Proposal and the Supporting Statement that the goal is to engage the Company in a discussion of its role in society as a critical player in the protection of privacy rights. To read the proposal otherwise is to twist the language of the Proposal.

The Company asserts that the Proposal is excludable as affecting its litigation strategy and the discovery process of numerous proceedings.[5] 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 social policy issues presented by the issue of disclosing customer information and communications to the authorities. 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.

With respect to the Company's argument concerning discovery, its argument is misplaced. First, the Company does not explain how a report that discusses the technical, legal and ethical policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers would circumvent discovery. Even assuming that, as permitted in the proposal, confidentiality prohibited any discussion of technical and legal policy issues (a point that we do not concede), how is it that a report which discusses the ethical policy issues raised by such disclosures would circumvent the discovery process? The Company has not pointed to any ethical policy issues that are raised in these lawsuits and we are unable to find ethical policy issues to be a part of the plaintiff's case or the defenses raised in these lawsuits. Clearly then at the very least, the Company could issue a report that discusses the social policy issues confronted by the Company from an ethical standpoint. While we believe the report could go farther and remain well within the parameters of the Rule, we believe even such a report would provide shareholders valuable information that allows them, in the words of the *Amalgamated Clothing and Textile Workers Union* court, "to communicate with other shareholders and with management. . . on matters of broad social import...." *Id*

---

5 Last year the Company attempted to cloud the facts of this case by insinuating that Mr. Jeremy Kagan's role as a proponent somehow tainted our efforts. Despite the fact that Mr. Kagan is not a proponent this year, the Company attempts to tie Mr. Kagan to the Proposal in footnote 12. We urge the Staff to disregard this distraction.

at 892. Consequently, the Company has not met its high burden under Rule 14a-8(g) of demonstrating that it is entitled to exclude the Proposal.

Turning now to the no-action letters cited by the Company it is evident that they do not apply to this case. *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 a social 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 social policy discussion of privacy rights in the context of disclosing customer information without a warrant 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, the 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 defend a suit in a given way, 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, inter alia, 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 excludable 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 and very significant social policy issues confronting the Company at this time and therefore is permissible under the Rule.

2. Customer Privacy: It is permissible to focus on privacy rights.

The Company further argues that the Proposal should be excluded because it improperly relates to customer privacy. Once again the Company's argument is misplaced because it mischaracterizes the Proposal as narrowly focused on the intricate details of AT&T's published privacy policies. As indicated before, the Proposal is focused on the broad and very significant social policy issues related to privacy rights confronting the Company at this time. Consequently, the no-action letters cited by the Company are not on point.

With respect to *Bank of America Corp.* (February 21, 2006) and (March 7, 2005), those cases are different than the Proposal because they requested a rote cataloging of *existing* procedures for ensuring confidentiality. This Proposal, in contrast, goes beyond such a day-to-day issue, and requests a discussion of the social policy issues. We observe that such a report could involve a discussion of potential future/additional procedures depending on how the Company sought to present the discussion. Our Proposal, however, does not simply focus on a mundane matter like describing existing procedural issues, but rather focuses on the significant policy issues of the societal concerns facing the Company as the result of the public and legal allegations relating to the Programs.[6]

A similar conclusion must be reached with respect to *Citicorp* (January 8, 1997) which was excluded for "monitoring illegal transfers through customer accounts". Specifically, that proposal sought a review of existing monitoring procedures with respect to an obscure issue which the proponent did very little to document how it was a significant social policy issue. As such, *Citicorp* is not applicable.

In *Verizon Communications Inc.* (February 22, 2007), the distinguishing feature of that proposal is that it included a focus on the issue of private individuals using pretexting to circumvent specific company procedures. Finally, addressing *Applied Digital Solutions, Inc.*, a review of that Staff letter shows the proposal was excluded because it related to "product development". Consequently, *Applied Digital Solutions, Inc.* is not relevant to this discussion and cannot be a basis for exclusion.

We respectfully suggest that the following cases are analogous to the Proposal:

---

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

In *Cisco Systems Inc.* (July 13, 2002), 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 . . .

Like *Cisco*, the Proposal seeks to address the significant privacy issues that the company faces. 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. As in *Cisco*, the proper conclusion is that the proposal is not excludable and properly raises significant policy issues that are appropriate for shareholders to consider. See also *Yahoo! Inc.*, (April 13, 2007) (shareholder proposal which requests that the company's management implement policies with certain minimum standards to help protect freedom of access to the Internet, may not be omitted from the company's proxy material under rule 14a-8(i)(3), (i)(6), (i)(7) or (i)(10)).

For the reasons set forth above, we request the Staff conclude that the Proposal is permissible.

3. Legal Compliance: the Proposal is not focused on legal compliance, but rather on social policy issues.

In contrast to the 2007 Proposal, the current Proposal is completely free of any references to compliance programs. For example, in the 2007 Proposal it could have been argued that the request for a report on "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" was inappropriately focused on legal compliance issues. In the 2008 Proposal, however, this language has been completely removed. What remains is a request to discuss the significant social policy issues facing the Company. In no way is this discussion dependent on a discussion of legal compliance as we have seen excluded in other cases. In fact, the Proposal specifically provides for an exclusion of information related to regulatory and litigation issues. Consequently in the unlikely event that compliance issues arise in the preparation of the report, they could be excluded by the Company.

Reviewing the no-action letters presented by the Company it is also evident that they do not apply. First, 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". The *Allstate* 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 requests a discussion on social policy issues. Second, the *Allstate* proposal sought a very 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 need to hire specific personnel to staff the committee. The Proposal in contrast is not even impliedly interested in those intricate details and plainly focuses on the significant social policy issues facing the Company.

In *Duke Power Company* (February 16, 1999) the shareholder sought very 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 the Proposal to *Duke* for the very simple reason that the *Duke* proposal achieved a extraordinary level of micro-management in a very highly regulated aspect of pollution controls. The Proposal in contrast deals with a high policy level discussion of privacy rights in the context of disclosing customer information without a warrant.

The *Halliburton Company* (March 10, 2006) proposal 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 sought a report on existing policies and focused on specific violations of federal law.

Finally, in *Monsanto Company* (November 3, 2005) the 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 sum, the Proposal does not seek to interfere in the day-to-day business of compliance programs and as a consequence does not qualify for the ordinary business exclusion.

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

The Company also 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".

Reviewing other no-action letter requests, it is also evident that some proposals which arguably 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.) Therefore, we urge the Staff to conclude the Proposal is not excludable as ordinary business.

5. "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 this argument, 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 next 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 in the context of disclosing customer information without a warrant 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.

Johnson & Johnson (February 7, 2003); *H.J. Heinz Co.* (May 25, 2001); and *Kohl's Corp.* (March 13, 2001) all were excluded because the shareholders were seeking implementation or reports based on a set of third party standards that were either not sufficiently defined in the proposal or were unknown to the company or its shareholders. This distinction is critical because there was no reason to assume that the shareholders in those cases were familiar with the third party standards, let alone what the details encompass. In contrast, it is reasonable to concluded that shareholders are familiar with the concept of privacy rights and have a reasonable understanding of that term that is essentially consistent from shareholder to shareholder.

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* are 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 resolved 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 social policy issue we would like to see the Company address. The issue is 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 is not applicable to the Proposal.

In contrast to the cases cited by the Company, there are numerous cases in which proposals were not excluded as being so vague as to make implementation impossible. Those cases are analogous to the Proposal.

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. See also *Yahoo!* (April 16, 2007).

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. 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), 14a-8(i)(6) and 14a-9 do not apply and cannot be a basis for excluding the Proposal.

IV. AT&T's privacy policies for customers are not substantial implementation of the Proposal.

The Company claims that the Proposal's request has been substantially implemented through the privacy policies it publishes on its website. However, based on a review of the website and the applicable no-action letters issued by the Staff it is clear that the Company has not met the Rule 14a-8(i)(10) standard because the websites:

- do not address the technological, legal or ethical issues raised by the Proposal;
- are excessively vague;
- are conclusory and therefore do not contain a discussion of the issues; and
- are not presented in a uniform fashion for a shareholder audience as requested.

Consequently, we believe the Proposal cannot be excluded as substantially implemented.

First, the content of the privacy policy clearly does not address the concerns raised by the Proponent. The privacy policy provided by the Company in Company Appendix 8 makes only cursory and conclusory mention of when AT&T would disclose customer information and makes no mention about disclosing communications content.

What we have requested is a *discussion* and that implicitly calls for a presentation of differing ideas and approaches. It means offering up for consideration what other companies have done in the past or are proposing to do. *The Proposal does not ask for a specific result or policy, but an exploration of the issues in the context of disclosing customer information without a warrant as they apply to the Company's future as a profitable and responsible company.* Clearly AT&T's privacy policy does not do that. The policy contained in the Company's Appendix 8 is far removed from a discussion of the social policy issues raised by the allegations from a technological, legal or ethical standpoint. In fact there is

no discussion of the technological or ethical policy issues surrounding disclosure in the Company's policy.

Furthermore, the privacy policy is intended to communicate information to *customers* while the Proposal requests information for *shareholders*. This is not a minor distinction. The concerns of shareholders can be very different than the concerns of its customers. For example, it would be nonsensical to discuss the ethics of privacy rights in a customer privacy policy statement published on a website. But given the widespread concern over these issues, it is important to shareholders to see that management has explored the technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content.

Second, the websites do not present the information in the same form as we request. The Proposal asks for a single report that contains the discussion. While the Company cites to one privacy policy, we observe that there are other privacy policies under the umbrella of AT&T. For example, there is a separate and distinct privacy policy at http://www.wireless.att.com/privacy/. We are asking the Company to provide shareholders with management's discussion in a unified manner, rather than over multiple websites perhaps containing duplicative and conclusory statements. In this regard consider *Newell Rubbermaid Inc.* (February 21, 2001) in which the Staff required inclusion of a proposal requesting that the board prepare a report on the company's "glass ceiling" progress, including a review of specified topics. The company claimed that it had already considered the concerns raised in the proposal and that it had publicly available plans in place. Despite those arguments, it was beyond dispute that the company had not prepared a report on the topic. Similarly, while the Company may argue that it has indirectly done what we ask, it has not provided documentation in a single report that substantially covers the issues.

Finally, it is important to observe that while AT&T is correct to cite many cases for the conclusion that companies are required to "substantially implement" proposals rather than "fully implement" proposals, what is critical is that it must, at the very least, address the core concerns raised by the proposal. See *Dow Chemical Company* (February 23, 2005); *ExxonMobil* (March 24, 2003); *Johnson & Johnson* (February 25, 2003); *ExxonMobil* (March 27, 2002); and *Raytheon* (February 26, 2001). In all of these cases the Staff rejected company arguments and concluded that the company's disclosures were insufficient to meet the substantially implemented standard. The case of *Wendy's International* (February 21, 2006) provides a particularly comparable example of the Staff rejecting a company's argument that information provided on a website was sufficient. In *Wendy's* the company argued that it had provided the requested sustainability report on its website and that the information contained on the website was sufficient. The proponent successfully demonstrated that the website contained no documentation that a discussion of the issues, as requested, had occurred and that the website only contained "vague statements of policy." Similarly, the company has not demonstrated that it has engaged in the discussion requested and the information on the Company's privacy policy websites is very general, i.e. does not address the numerous core issues raised in the Proposal. Consequently, we respectfully request that the Staff not concur with the Company and not permit it to exclude the Proposal on Rule 14a-8(i)(10) grounds.

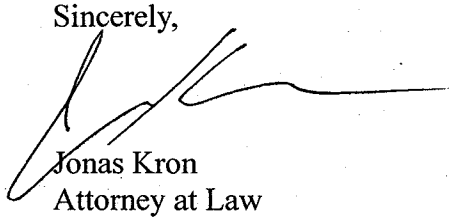
Conclusion

In conclusion, we respectfully request the Staff to inform the Company that Rule 14a-8 requires a denial of the Company's no-action request. As demonstrated above, the Proposal is not excludable

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. These issues are being discussed already in public and they are properly raised in our company's proxy. In the event that the Staff should decide to concur with the Company and issue a no-action letter, we respectfully request the opportunity to speak with the Staff.

Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information. Also, pursuant to Staff Legal Bulletin No. 14 B, section F.3. we request the Staff fax a copy of its response to the Proponents at (801) 642-9522.

Sincerely,



Jonas Kron
Attorney at Law
Attorney for the Proponents

Enclosures

cc: Paul Wilson, Senior Attorney, Legal Department, AT&T Inc.

Appendix A

As You Sow
Planting Seeds for Social Change

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

November 20, 2007

Randall L. Stephenson,
Chairman and Chief Executive Officer
AT&T Inc.
175 E. Houston
San Antonio, TX 78205

Re: Shareholder Resolution on Privacy Policy

Dear Mr. Stephenson,

As a shareholder of AT&T, and the Executive Director of As You Sow, I am concerned about reports that AT&T provided customer information to the National Security Agency without a warrant. I 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 shareholders on the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. It could also have an impact on the share price which may be affected by potential legal liabilities.

Therefore, I am co-filing, with Calvert Asset Management Company and the Adrian Dominican Sisters, the enclosed shareholder proposal for inclusion in the 2008 proxy statement. This filing is in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities Exchange Act of 1934.

I have been an AT&T shareholder continuously for many years and will continue to hold the shares through the 2008 stockholder meeting. I, or my representative, will attend the stockholders' meeting to move the resolution.

Sincerely,

Larry Fahn

Shipment Receipt: Page #1 of 1

THIS IS NOT A SHIPPING LABEL. PLEASE SAVE FOR YOUR RECORDS

SHIP DATE:
Tues, Nov 20, 2007

EXPECTED DELIVERY DATE:
WED, NOV 21, 2007 3:00 PM

SHIP FROM:
Jonas Kron
2940 SE Woodward St.
Portland, OR 97202
(971) 222-3366

SHIP TO:
RANDALL L STEPHENSON, CEO
AT&T INC
175 E HOUSTON
SAN ANTONIO TX 78205-2255
Business

SHIPPED THROUGH:
The UPS Store #3234
PORTLAND, OR 97214
(503) 236-5687

SHIPMENT INFORMATION:
UPS Next Day Air Saver Com
0.14Lbs / LTR Billed Weight
Carrier Letter

Tracking Number: 1ZE3F3311397107388
Shipment ID: MYVD4O3XPZM8D
Or/Item#: 23262671
Ref#: 23262671

DESCRIPTION OF GOODS:
DOCUMENTS

SHIPMENT CHARGES:

Next Day Air Saver Com	$20.20
Service Options	$0.00
Fuel Surcharge	$3.33
Total	$23.53

[illegible]

Signature:

ShipmentID: MYVD4O3XPZM8D

[illegible]

*** FISMA & OMB Memorandum M-07-16 ***

Appendix B

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, et al,

Plaintiffs,

v

AT&T CORPORATION, et al,

Defendants.
_____/

No C-06-672 VRW

ORDER

Plaintiffs allege that AT&T Corporation (AT&T) and its holding company, AT&T Inc, are collaborating with the National Security Agency (NSA) in a massive warrantless surveillance program that illegally tracks the domestic and foreign communications and communication records of millions of Americans. The first amended complaint (Doc #8 (FAC)), filed on February 22, 2006, claims that AT&T and AT&T Inc have committed violations of:

(1) The First and Fourth Amendments to the United States Constitution (acting as agents or instruments of the government) by illegally intercepting, disclosing, divulging and/or using plaintiffs' communications;

(2) Section 109 of Title I of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 USC § 1809, by engaging in illegal electronic surveillance of plaintiffs' communications under color of law;

(3) Section 802 of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by section 101 of Title I of the Electronic Communications Privacy Act of 1986 (ECPA), 18 USC §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a), by illegally intercepting, disclosing, using and/or divulging plaintiffs' communications;

(4) Section 705 of Title VII of the Communications Act of 1934, as amended, 47 USC § 605, by unauthorized divulgence and/or publication of plaintiffs' communications;

(5) Section 201 of Title II of the ECPA ("Stored Communications Act"), as amended, 18 USC §§ 2702(a)(1) and (a)(2), by illegally divulging the contents of plaintiffs' communications;

(6) Section 201 of the Stored Communications Act, as amended by section 212 of Title II of the USA PATRIOT Act, 18 USC § 2702(a)(3), by illegally divulging records concerning plaintiffs' communications to a governmental entity and

(7) California's Unfair Competition Law, Cal Bus & Prof Code §§ 17200 et seq, by engaging in unfair, unlawful and deceptive business practices.

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

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

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

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

At a May 17, 2006, hearing, the court requested additional briefing from the parties addressing (1) whether this case could be decided without resolving the state secrets issue, thereby obviating any need for the court to review the government's classified submissions and (2) whether the state secrets issue is implicated by an FRCP 30(b)(6) deposition request for information about any certification that AT&T may have received from the government authorizing the alleged wiretapping activities. Based on the parties' submissions, the court concluded in a June 6, 2006, order that this case could not proceed and discovery could not commence until the court examined *in camera* and *ex parte* the classified documents to assess whether and to what extent the state secrets privilege applies. Doc #171.

After performing this review, the court heard oral argument on the motions to dismiss on June 23, 2006. For the reasons discussed herein, the court DENIES the government's motion to dismiss and DENIES AT&T's motion to dismiss.

I

The court first addresses the government's motion to dismiss or, alternatively, for judgment on state secrets grounds. After exploring the history and principles underlying the state secrets privilege and summarizing the government's arguments, the court turns to whether the state secrets privilege applies and requires dismissal of this action or immediate entry of judgment in favor of defendants. The court then takes up how the asserted privilege bears on plaintiffs' discovery request for any government certification that AT&T might have received authorizing the alleged

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

A

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

//

//

//

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

> 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.

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

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

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

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

//

//

//

//

> The privilege belongs to the Government and must be asserted by it * * *. It is not to be lightly invoked. 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. 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.

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

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

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

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

On certified appeal, the District of Columbia Circuit noted that even "seemingly innocuous" information is privileged if that information is part of a classified "mosaic" that "can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate." Id at 8. The court affirmed dismissal of the claims related to operation MINARET but reversed the district court's rejection of the privilege as to operation SHAMROCK, reasoning that "confirmation or denial that a particular plaintiff's communications have been acquired would disclose NSA capabilities and other valuable intelligence information to a sophisticated intelligence analyst." Id at 10. On remand, the district court dismissed plaintiffs' claims against the NSA and individuals connected with the NSA's alleged monitoring. Plaintiffs were left with claims against the Central Intelligence Agency (CIA) and individuals who had allegedly submitted watchlists to the NSA on the presumption that the submission resulted in interception of plaintiffs' communications. The district court eventually dismissed the CIA-related claims as well on state secrets grounds and the case went up again to the court of appeals.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B

Relying on Kasza, the government advances three reasons why the state secrets privilege requires dismissing this action or granting summary judgment for AT&T: (1) the very subject matter of 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.

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

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

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

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

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

//

//

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

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

C

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

//

1

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

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

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

> The activities I authorized are reviewed approximately every 45 days. Each review is based on a fresh intelligence assessment of terrorist threats to the continuity of our Government and the 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.

//

//

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

Id.

Attorney General Alberto Gonzales subsequently confirmed that this program intercepts "contents of communications where * * * one party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Doc #87 (AT&T Request for Judicial Notice), Ex J at 1 (hereinafter "12/19/05 Press Briefing"), available at http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html (last visited July 19, 2005). The Attorney General also noted, "This [program] is not about wiretapping everyone. This is a very concentrated, very limited program focused at gaining information about our enemy." Id at 5. The President has also made a public statement, of which the court takes judicial notice, that the government's "international activities strictly target al Qaeda and their known affiliates," "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.

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

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

> In the Fall of 2001 * * * while Mr Nacchio was Chairman and CEO of Qwest and was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee, Qwest was approached to permit the Government access to the private telephone records of Qwest customers.
>
> Mr Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a 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 Telecommications [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.

Markman Decl, Ex 6.

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

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

News Release, BellSouth Statement on Governmental Data Collection (May 15, 2006), available at http://bellsouth.mediaroom.com/index.php?s=press_releases&item=2860 (last visited July 19, 2006). Although declining to confirm or deny whether it had any relationship to the NSA program acknowledged by the President, Verizon stated in relevant part:

> One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.
>
> This is false. From the time of the 9/11 attacks until just four months ago, Verizon had three major businesses - its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of these businesses, or any call data from those records. None of these companies — wireless or wireline — provided customer records or call data.

See News Release, Verizon Issues Statement on NSA Media Coverage (May 16, 2006), available at 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

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

2

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

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

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

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

D

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

//

//

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

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

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

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

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

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

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

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

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

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

E

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

1

Although the principles announced in Totten, Tenet, Reynolds and Kasza inform the court's decision here, those cases are not strictly analogous to the facts at bar.

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

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

More importantly, unlike the clandestine spy arrangements in Tenet and Totten, 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. This program operates without warrants and targets "contents of communications where * * * one party to the communication is outside the United States" and the government has "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." 12/19/05 Press Briefing at 1.

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

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

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

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

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

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

//

//

//

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

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

2

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

//

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

//

//

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

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

3

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

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

4

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

F

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

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

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

//

//

//

//

//

//

//

//

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

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

3

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

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.

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

4

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

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

Nonetheless, the court is hesitant to conclude that the existence or non-existence of the communication records program necessarily constitutes a state secret. Confirming or denying the existence of this program would only affect a terrorist who was insensitive to the publicly disclosed "terrorist surveillance program" but cared about the alleged program here. This would seem unlikely to occur in practice given that the alleged communication records program, which does not involve listening in on communications, seems less intrusive than the "terrorist surveillance program," which involves wiretapping. And in any event, it seems odd that a terrorist would continue using AT&T given that BellSouth, Verizon and Qwest have publicly denied participating in the alleged communication records program and would appear to be safer choices. 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.

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

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

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

5

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

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

H

The government also asserts two statutory privileges in its motion to dismiss that it contends apply "to any intelligence-related information, sources and methods implicated by [p]laintiffs' claims and the information covered by these privilege claims are at least co-extensive with the assertion of the state secrets privilege by the DNI." Gov MTD at 14. First, the government relies on 50 USC § 402 *note*, which 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, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

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

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

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

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

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

//

//

//

//

//

//

//

//

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.

//

//

//

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

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

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

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

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

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

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

//

//

//

//

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

> Whether styled as a constitutional or prudential limit on standing, the Court has sometimes determined that where large numbers of Americans suffer alike, the political process, rather than the judicial process, may provide the more appropriate remedy for a widely shared grievance.
>
> [This] kind of judicial language * * * however, invariably appears in cases where the harm at issue is not only widely shared, but is also of an abstract and indefinite nature.

Id at 23. The Court continued:

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

Id at 24.

Here, the alleged injury is concrete even though it is widely shared. Despite AT&T's alleged creation of a dragnet to intercept all or substantially all of its customers' 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.

//

//

//

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

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

//

//

//

//

B

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

As discussed above, the procedural requirements for a certification are addressed in 18 USC § 2511(2)(a)(ii)(B). See *supra* I(G)(1). Under section 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." This provision is referenced in 18 USC § 2520(a) (emphasis added), which creates a private right of action under Title III:

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

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

> No cause of action shall lie in any court against 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.

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

> A civil action will not lie [under 18 USC § 2520] where the requirements of sections 2511(2)(a)(ii) of title 18 are met. With regard to that exception, the Committee intends that the following procedural standards will apply:
>
> > (1) The complaint must allege that a wire or electronic communications service provider (or one of its employees) (a) disclosed the existence of a wiretap; (b) acted without a facially valid court order or certification; (c) acted beyond the scope of a court order or certification or (d) acted on bad faith. Acting in bad faith would include failing to read the order or collusion. If the complaint fails to make any of these allegations, the defendant can move to dismiss the complaint for failure to state a claim upon which relief can be granted.

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

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

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

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

> 81. On information and belief, the above-described acts [by defendants] of interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications occurred without judicial or other lawful authorization, probable cause, and/or individualized suspicion.
>
> 82. On information and belief, at all relevant times, the government instigated, directed and/or tacitly approved all of the above-described acts of AT&T Corp.

FAC, ¶¶ 81-82 (emphasis added).

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

> The emphasis there is on the word 'lawful[.'] When 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.

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

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

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

//

//

C

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 (DDC 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:

//

//

//

//

//

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

Id at 846.

Smith v Nixon involved an allegedly illegal wiretap that was part of the same surveillance program implicated in Halperin. In addressing C&P's potential liability, the Smith court noted:

> The District Court dismissed the action against C&P, which installed the wiretap, on the ground cited in the District Court's opinion in Halperin: 'C&P's limited technical role in the surveillance as well as its reasonable expectation of legality cannot give rise to liability for any statutory or constitutional violation. * * *.' We think this was the proper disposition. The telephone company did not initiate the surveillance, and it was 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.

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

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

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

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

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

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

Craska also does not help AT&T. In that case, plaintiff sued a telephone company for violating her statutory rights by turning over telephone records to the government under compulsion of state law. Craska, 239 F Supp at 933-34, 936. The court declined to ascribe any liability to the telephone company because its assistance was required under state law: "[T]he conduct of the telephone company, acting under the compulsion of State law and process, cannot sensibly be said to have joined in a knowing venture of interception and divulgence of a telephone conversation, 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

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

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

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

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

D

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

//

//

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

1

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

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

Applying Wyatt to a case involving section 1983 claims against privately employed prison guards, the Supreme Court in Richardson v McKnight, 521 US 399 (1997), stated that courts should "look both to history and to the purposes that underlie government employee immunity in order to" determine whether that immunity extends to private parties. Id at 404. Although this issue has been addressed by the Ninth Circuit in several cases, the court has yet to extend qualified immunity to a private party under McKnight. 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.

//

//

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

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

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

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

federal constitutional violations); Maine v Thiboutot, 448 US 1 (1980) (holding that section 1983 could be used to vindicate non-constitutional statutory rights); Harlow, 457 US at 818 (making the unprecedented reference to "clearly established statutory" rights just two years after Thiboutot (emphasis added)). These causes of action "were devised by the Supreme Court without any legislative or constitutional (in the sense of positive law) guidance." Crawford-El v Britton, 93 F3d 813, 832 (DC Cir 1996) (en banc) (Silberman concurring), vacated on other grounds, 523 US 574 (1998). "It is understandable then, that the Court also developed the doctrine of qualified immunity to reduce the burden on public officials." Berry, 146 F3d at 1013.

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

//

//

Similarly, Congress specifically contemplated that communications carriers could be liable for violations of Title III. See Jacobson, 592 F2d at 522. And in providing for a "good faith" defense in Title III, Congress specifically sought "'to protect telephone companies or other persons who cooperate * * * with law enforcement officials.'" Id at 522-23 (quoting Senate debates). See also id at 523 n 13. Cf 18 USC § 2511(2)(a)(ii) (providing a statutory defense to "providers of wire or electronic communication service").

In sum, neither the history of judicially created immunities for telecommunications carriers nor the purposes of qualified immunity justify allowing AT&T to claim the benefit of the doctrine in this case.

3

The court also notes that based on the facts as alleged in plaintiffs' complaint, AT&T is not entitled to qualified immunity with respect to plaintiffs' constitutional claim, at least not at this stage of the proceedings. Plaintiffs' constitutional claim alleges that AT&T provides the government with direct and indiscriminate access to the domestic communications of AT&T customers. See, e g, FAC, ¶ 42 ("On information and belief, AT&T Corp has provided and continues to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities, including direct access to streams of domestic, international and foreign telephone and Internet communications."); id, ¶ 78 (incorporating paragraph 42 by reference into plaintiffs'

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

4

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

//

//

//

III

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

//

//

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

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

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

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

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

//

//

//

//

//

//

//

//

//

//

//

//

//

IV

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

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

IT IS SO ORDERED.

VAUGHN R WALKER
United States District Chief Judge

Appendix C

*** FISMA & OMB Memorandum M-07-16 ***

Media Reports on the Programs

Print and Electronic

1. Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 11, 2006

2. Victoria Toensing, *Constitutional Surveillance,* The Weekly Standard, March 6, 2006.

3. John O'Neil and Eric Lichtblau, *Qwest's Refusal of N.S.A. Query Is Explained,* New York Times, May 12, 2006

4. Ken Belson and Matt Richtel, *Verizon Denies Turning Over Local Phone Data,* The New York Times, May 17, 2006

5. Matt Richtel and Ken Belson, *U.S. Focused on Obtaining Long-Distance Phone Data, Company Officials Indicate*, New York Times, May 18, 2006

6. Evan Hansen, *Why We Published the AT&T Docs*, Wired News, May 22, 2006

7. Michael Higgins, *ACLU Sues AT&T Over Phone Records*, Chicago Tribune, May 20, 2006

8. Anthony D. Romero, *A Little Straight Talk, Please, on the NSA Scandal*, Salt Lake Tribune, May 20, 2006

9. Marcia Coyle, *The Fight Over Phone Records*, National Law Journal, May 22, 2006

10. Studs Terkel, *Other Sue AT&T Over Release of Records*, Associated Press, May 23, 2006

11. Larry Neumeister, *ACLU Seeks to Rally Population Against Govt's Phone Snooping*, Associated Press, May 23, 2006

12. Peter Grier, *For Telecoms, a Storm of Lawsuits Awaits*, Christian Science Monitor, May 24, 2006

13. Larry Neumeister, *ACLU Files Complaints Over Government Phone Snooping*, Associated Press, May 25, 2006

14. Editorial, *Make No Law*, Washington Post, May 25, 2006

15. Ryan Kim, *INSECURITY: Bugged by Phone Companies*, San Francisco Chronicle, May 25, 2006

16. Kathleen Burge, *Mayors Demand Phone Inquiry*, Boston Globe, May 25, 2006

17. Michael D. Sorkin, *AT&T Broke Privacy Laws, Suit Here Says*, St. Louis Post-Dispatch (Missouri), May 25, 2006

18. Darren M. Allen, *ACLU Files Complaint Over Phone Records*, Rutland Herold (Vermont), May 25, 2006

19. Paul Shukovsky, *ACLU in State Wants Phone Firms Checked*, Seattle Post Intelligencer, May 25, 2006

20. Ian Martinez, *ACLU Attacks Wiretapping at State Level*, Communications Daily, May 25, 2006

21. Mary Schmich and Eric Zorn, *Is it a Big Deal if the Feds Have Your Number?*, Chicago Tribune, May 25, 2006

22. John Diamond, *Specter: Cheney put pressure on panel*, USA Today, June 7, 2006

23. John Diamond, *Senators won't grill phone companies*, USA Today, June 7, 2006

24. Ryan Singel, *AT&T: Wired News Is a 'Scofflaw'*, Wired News, June 13, 2006

25. Scott Lindlaw, SF Reviews Contracts with AT&T Over Domestic Spying, Associated Press, July 11, 2006

26. Ryan Singel, *Judge: NSA Case Can Proceed*, Wired News, July 20, 2006

27. Roger Cheng, *Judge Denies AT&T, U.S. Motion to Dismiss Domestic Spying Case,* Wall Street Journal, July 21, 2006

28. Declan McCullagh, *AT&T says cooperation with NSA could be legal*, CNET News.com, August 22, 2006

29. Katie Zezima, *Maine: Lawsuit Over Phone Records*, New York Times, September 22, 2006

30. Ryan Singel, *NSA Case Becomes Lawyer Junket*, Wired News, November 17, 2006

31. Declan McCullagh, *Judge won't halt AT&T wiretapping lawsuit*, CNET News.com, November 18, 2006

32. Onnesha Roychoudhuri, *DoJ Quashes Wiretapping Inquiries*, In These Times (Illinois) November 20, 2006

33. 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

*** FISMA & OMB Memorandum M-07-16 ***

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. Nothwithstanding 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 agencies[1] ("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 theses 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 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 authorization . . . .[42]

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. *Terkel*at 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; *Terkel*at 5, 21.

85. *Terkel*at 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 issued 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. *Terkel*at 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 requires 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 State. 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.

s/ James Volz)
)
) PUBLIC SERVICE
)
s/ David C. Coen) BOARD
)
) OF VERMONT
s/ John D. Burke)

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 J. 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 agency[4] 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 employe access to customer information and the purposes for which this information may be used by employes 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

Paul M. Wilson
Senior Attorney
Legal Department
175 E. Houston, Room 222
San Antonio, Texas 78205
(210) 351-3326

1934 Act/ Rule 14a-8

January 18, 2008

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. 2008 Annual Meeting – Shareholder Proposals of Adrian Dominican Sisters and Calvert Asset Management

Ladies and Gentlemen:

We refer to the recent letter, dated January 7, 2008, from Jonas D. Kron, on behalf of Larry Fahn, Calvert Asset Management Company, Inc. ("Proponent Calvert") and the Adrian Dominican Sisters ("Proponent ADS," and together with Proponent Calvert and Larry Fahn, "Proponents") asking the Staff not to concur in AT&T Inc.'s ("AT&T" or the "Company") conclusion, as described in our letter to you of December 18, 2007, that AT&T may omit the shareholder proposal submitted by Proponent Calvert (the "Calvert Proposal") and the shareholder proposal submitted by Proponent ADS (the "ADS Proposal") from the proxy statement for its 2008 Annual Meeting.

Pursuant to Rule 14a-8(j), enclosed are six copies of this letter and the confirming opinion of Sidley Austin LLP. Copies of this letter and the confirming opinion of Sidley Austin LLP are also being mailed concurrently to Jonas D. Kron.

This letter addresses the issues raised by Mr. Kron in his January 7, 2008 letter and should be read in conjunction with AT&T's original letter to the Staff, dated December 18, 2007.

Mr. Kron's extensive letter objects to AT&T's exclusion of the Proposals on each of the grounds asserted by the Company. 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 18th letter. Nevertheless, we set forth below our general views regarding Mr. Kron's letter.

The Proposals May be Omitted Pursuant to Rules 14a-8(b), 14a-8(f) and 14a-8(e) Because Proponents Failed to Establish their Eligibility to Submit the Proposals.

Mr. Kron argues that Proponent Calvert's ownership eligibility under Rule 14a-8(b) is substantiated by a combination of a letter from State Street Corp., dated December 3, 2007, (the "State Street Letter") stating that Proponent Calvert's funds held the requisite AT&T shares as of November 20, 2007 and Proponent Calvert's own letter, dated December 6, 2007, asserting that its funds have held these shares continuously for at least one year prior to the date it submitted the Calvert Proposal.[1] According to Mr. Kron, it is "the December 3rd State Street letter and the clear language of Calvert's December 6, 2007 letter [that] make it evident that Calvert has owned the requisite shares for a continuous period of time in excess of one year prior to submission." As discussed more fully in AT&T's December 18th letter, the State Street Letter is defective in that it both fails to indicate the date as of which Proponent Calvert held its AT&T shares continuously for one year and references a date that does not correspond to the date the Calvert Proposal was submitted. Contrary to Mr. Kron's position, nothing in Proponent Calvert's own letter to the Company can properly serve to cure the defective State Street Letter since statements from a beneficial owner about its stock ownership cannot, in any event, serve to satisfy the Commission's regulatory requirements for *independent* corroborative proof of continuous share ownership. Rule 14a-8(b) requires a proponent to corroborate its ownership eligibility by providing either a written statement from the record holder of the securities or copies of Commission filings, and the Staff has made clear on numerous occasions that assertions by a putative beneficial owner as to its own share ownership and/or the required holding period for such shares cannot service to establish the proof required by Rule 14a-8(b). *See Staff Legal Bulletin No. 14 (CF)* (July 13, 2001); *AT&T Corp.* (January 24, 2001); *International Business Machines Corp.* (December 16, 1998); *International Business Machines Corp.* (December 7, 2007).

With respect to the eligibility of Proponent ADS, rather than addressing AT&T's arguments directly, Mr. Kron asserts only that "[i]t is also clear from a common sense reading of ADS's reply to the Company's deficiency letter that ADS continued to own the shares at that time and would continue to do so through the Annual Meeting." However, Mr. Kron fails to point out where in either the letter or the bank statements from Comerica Bank - the record holder of Proponent ADS's AT&T shares (the "Comerica Bank Letters") – it clearly states that the requisite shares were held *continuously* for one year prior to submission of the ADS Proposal. The Comerica Letters read: "[T]he above referenced account currently

[1] A copy of Proponent Calvert's letter, dated December 6, 2007, and the attached State Street Letter is attached as Appendix 6 to AT&T's original letter to the Staff, dated December 18, 2007.

holds [ ] shares of AT&T common stock. The attached list indicates the date the stock was acquired."[2] Contrary to Mr. Kron's cursory conclusion, continuous ownership is not evident from any reading of the Comerica Letters or the attached bank statements. Furthermore, Mr. Kron completely ignores AT&T's argument that the Comerica Letters are defective in that they do not establish that Proponent ADS held the requisite amount of AT&T shares continuously for one year *as of the date the ADS Proposal was submitted.*

The Commission's rules with respect to ownership eligibility are clear and have been carefully designed to ensure that proper proof of beneficial ownership is timely furnished to a company. The Staff has made clear the need for precision in the context of demonstrating a shareholder's eligibility under Rule 14a-8(b) so that neither the company nor the Commission would be required to speculate as to whether all of the requirements have been met. As discussed at length in AT&T's December 18th letter, neither Proponent Calvert nor Proponent ADS has clearly demonstrated its ownership eligibility as required under Rule 14a-8(b).
The proposal of Larry Fahn (the "Fahn Proposal," and together with the Calvert Proposal and the ADS Proposal, the "Proposals") can likewise be excluded for lack of eligibility under Rule 14a-8(e)(2). Under Rule 14a-8(e)(2), in order for a shareholder proposal to be eligible for inclusion in a company's proxy materials, the proposal must be received at the company's principal executive offices not less than 120 calendar days before the proxy statement is released to shareholders. AT&T's 2007 proxy statement specifically provides that shareholder proposals submitted for inclusion in the proxy materials for the 2008 annual meeting "must be received by AT&T...by November 23, 2007. Such proposals should be sent in writing by certified mail *to the Senior Vice President and Secretary* of AT&T" (emphasis added). AT&T requires shareholder proposals to be sent in this manner because it has established internal controls to ensure that shareholder proposals addressed in this way are properly routed to the appropriate people within the Company.

Contrary to AT&T's explicit instructions, the Fahn Proposal was addressed to the Chairman and Chief Executive Officer. While the Company takes steps to insure that shareholder proposals addressed to the Chairman and Chief Executive Officer or other members of management are forwarded promptly to the Senior Vice President and Secretary, given that the Chairman and Chief Executive Officer receives up to 100 pieces of mail each day, on occasion an item may be mishandled, as in Mr. Fahn's case. This is precisely why we instruct shareholders to address their proposals to the Senior Vice President and Secretary. Because the Fahn Proposal was improperly addressed, it did not reach the Corporate Secretary by the November 23rd submission deadline and is thus ineligible for inclusion in the Company's 2008 proxy materials.

---

[2] Copies of the six Comerica Letters and the attached bank statements are attached as Appendix 1 to AT&T's original letter to the Staff, dated December 18, 2007.

In New York Community Bancorp., a shareholder proposal that was addressed to the company's chairman was sent by facsimile to the company's principal executive offices four days before the deadline, but due to a clerical error the proposal was not forwarded to the corporate secretary. The Staff concurred with the company that the proposal could be omitted from its proxy materials under Rule 14a-8(e)(2) because the proposal was not received before the submission deadline. *New York Community Bancorp.* (August 8, 2007). Numerous other no-action precedents indicate the Staff's willingness to exclude improperly addressed shareholder proposals. See, e.g. *Xerox Corporation* (May 2, 2005); *Coca-Cola Co.* (January11, 2001); *Nabors Industries Ltd.* (April 15, 2003); *Intel Corporation* (March 5, 2004); *WorldCom, Inc.* (March 7, 2001). As in all of these examples, the Fahn Proposal failed to reach AT&T's Corporate Secretary by the submission deadline because it was improperly addressed and can therefore be excluded under Rule 14a-8(e)(2). The fact that the Company did not notify Mr. Fahn of this deficiency is of no consequence since, as provided in Rule 14a-8(f)(1), where a deficiency cannot be remedied (such as failure to submit a proposal by the deadline), the company is not required to provide notice of it.

Moreover, because the Fahn Proposal is identical to the Proposals submitted by Proponent ADS and Proponent Calvert, we believe that all of the substantive arguments for excluding those Proposals made in our December 18th letter, as well as the arguments made in this letter, likewise apply to the Fahn Proposal. Therefore, the Fahn Proposal can also properly be omitted for all of the reasons stated therein and below.

The Proposals May be Omitted Pursuant to Rule 14a-8(i)(2) Because Implementing the Proposals Would Cause AT&T to Violate Federal Law.

Mr. Kron's arguments against exclusion of the Proposals under Rule 14a-8(i)(2) lack merit because they fail 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 Appendix 7 to AT&T's December 18th letter (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 Proposals in order to make them seem more innocuous. Mr. Kron's arguments do nothing to contradict our original position that implementing the Proposals would cause AT&T to violate the law. Having considered the arguments made in Mr. Kron's letter, Sidley Austin has nevertheless confirmed its earlier opinion that implementing the Proposals would cause the Company to violate numerous

federal laws in a confirming opinion dated January 10, 2008 (the "Confirming Sidley Austin Opinion").[3]

Furthermore, Mr. Kron emphasizes the fact that AT&T did not cite any specific no-action precedents in its December 18th letter to support its argument that the Proposals can be properly omitted under Rule 14a-8(i)(2). This argument is irrelevant to a determination that the Proposals are properly excludable. Both the Sidley Austin Opinion and the Confirming Sidley Austin Opinion clearly illustrate that implementing the Proposals would cause AT&T to violate a series of federal laws designed to protect the intelligence gathering activities of the United States and cite ample compelling legal authority to support that conclusion. This showing – that a proposal would, if implemented, cause the company to violate any state, federal or foreign law to which it is subject – is all that is required in order to properly omit a shareholder proposal under Rule 14a-8(i)(2).

The Proposals May be Omitted Pursuant to Rule 14a-8(i)(7) Because They Relate to Ordinary Business Matters.

The Proposals relate to ordinary business matters and do not implicate any significant public policy concerns.

Mr. Kron's arguments with respect to the Proposal's "substantial policy considerations" mischaracterize the magnitude of the privacy concerns purported to be implicated by the Proposals. 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. In fact, in response to AT&T's letter to the Staff, dated December 11, 2006, regarding its intention to omit a substantially similar proposal co-sponsored by the Proponents, Mr. Kron wrote a lengthy letter arguing that the proposal raised significant social policy issues and citing a laundry list of examples like the ones found in his current letter. The Staff nonetheless concluded that these policy considerations were not substantial and allowed the Company to exclude the proposal under Rule 14a-8(i)(7) as impermissibly relating to AT&T's ordinary business of managing its litigation strategy. *AT&T Inc.* (February 9, 2007). Mr. Kron has not indicated any reasons why the social policy issues discussed in his current letter are any more significant than those considered by the Staff last year.

The Staff reached similar conclusions in Verizon Communications Inc. and Bank of America Corp. and determined that any social policy concerns implicated by shareholder proposals substantially similar to the current Proposals were not significant enough to override management's legitimate need for overseeing the company's daily business operations. The policy considerations purportedly

[3] A copy of the Confirming Sidley Austin Opinion is enclosed with this letter as Exhibit 1.

implicated by the Proposals are no more "substantial" than those which the Staff considered in making its determination that both Bank of America and Verizon Communications could exclude substantially similar proposals under Rule 14a-8(i)(7). *Verizon Communications Inc.* (February 22, 2007); *Bank of America Corp.* (February 21, 2006); *Bank of America Corp.* (March 7, 2005). Although Mr. Kron cites Cisco Systems Inc. as support for his position, he conveniently ignores the numerous no-action 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) (in both cases, 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 Proposals relate to ongoing litigation involving the Company.

Mr. Kron's objection to AT&T's argument that the Proposals relate to the Company's ongoing litigation is that the Proposals do not "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." This, however, is not the proper standard for exclusion. As Mr. Kron rightly points out, the correct standard 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 Proposals satisfy this standard. As discussed at length in AT&T's December 18th letter and the Sidley Austin Opinion, the report called for by the Proposals necessarily requires a discussion of the very same matters which are at the very heart of the multiple pending lawsuits and other proceedings that AT&T is currently defending. Compliance with the Proposals would require the Company to produce information that goes directly to the substance of these lawsuits and other proceedings, thereby sidestepping and interfering with the discovery process in these actions.

In fact, as discussed above, the Staff has already excluded a substantially similar proposal, co-sponsored by Proponents, on the ground that it related to AT&T's litigation strategy. *AT&T Inc.* (February 9, 2007). Although Mr. Kron attempts to re-characterize the current Proposals in more innocuous terms, the Proposals are substantially similar to the proposal permitted to be excluded in 2007. Like that proposal, the type of discussion sought by the current Proposals necessarily requires the Company to provide information that is central to the multiple pending lawsuits and other proceedings in which AT&T is currently involved.

Thus, the Proposals would compromise AT&T's litigation strategy, even though they might not direct any particular result or require the Company to divulge its strategies, as Mr. Kron claims.

The fact that the Proposals specifically allow the Company to exclude "confidential information, including information that would reveal the Company's litigation, regulatory or lobbying strategy" does not mitigate the applicability of Rule 14a-8(i)(7)'s exclusions for proposals relating to a company's ongoing litigation. Regardless of the Proposals' permitted exclusions, the subject matter of the Proposals is clearly the same or similar to the subject matter of AT&T's current litigation. If the Company excludes from the report required by the Proposals all information that is confidential and/or reveals the Company's litigation strategy, along with all of the other types of information also permitted to be excluded by the Proposals, the report would contain no substantive information and would mean that the Proposals are inherently impossible to implement.

Mr. Kron's lengthy discussion of the technical distinctions between the no-action precedents cited by AT&T and the Proposals fails to appreciate the fact that these precedents were cited simply as an illustration of the Staff's standard for exclusion of shareholder proposals as relating to the company's ongoing litigation. Applying Mr. Kron's own analysis, each of the no-action precedents he cites in support of his position can likewise be distinguished from the Proposals at issue here.

The Proposals relate to matters of customer privacy.

Mr. Kron argues that the Proposals are distinguishable from the proposals relating to matters of customer privacy permitted to be excluded in Bank of America Corp. and Verizon Communications Inc. because the Proposals "focus on the significant policy issues of the societal concerns facing the Company as the result of the public and legal allegations relating to" specified government surveillance programs. This distinction lacks merit. The Proposals, regardless of their perceived focus, essentially ask AT&T to produce a report discussing the disclosure of customer information to federal and state agencies and the effect of such disclosure on customer privacy, in response to an alleged breach of that privacy. In this way, the Proposals are virtually identical to those excluded in Bank of America Corp. and Verizon Communications Inc. *Verizon Communications Inc.* (February 22, 2007); *Bank of America Corp.* (February 21, 206); *Bank of America Corp.* (March 7, 2005).

Rather than distinguishing the Proposals in any meaningful way, Mr. Kron simply concludes that the Proposals should not be excluded on this basis because they request a discussion of social policy issues. However, Mr. Kron fails to

acknowledge that such a discussion would necessarily entail a discussion of matters of customer privacy and AT&T's policies and procedures for protecting that privacy. These matters are integral to the day-to-day business operations of a company such as AT&T, and, thus, proposals relating to such matters are properly excludable as relating to the Company's ordinary business matters.

The Proposals relate to matters of legal compliance.

In arguing that the Proposals do not relate to matters of legal compliance, Mr. Kron again mischaracterizes the Proposals as merely requesting a discussion of "the significant social policy issues facing the Company." However, the text of the Proposals and their Supporting Statements establishes that the Proposals seek to discover the relationship, if any, between AT&T and various state and federal agencies in response to allegations that the Company provided customer information to these agencies. A discussion of the technical, legal and ethical issues related to this alleged cooperation clearly relates to matters of the Company's legal compliance, and Mr. Kron's letter does not provide any evidence to the contrary. In this regard, the distinctions that Mr. Kron draws between the no-action precedents cited by AT&T in support of its argument and the Proposals are largely irrelevant.

While Mr. Kron correctly points out that the Proposals specifically provide for exclusion of information related to regulatory and litigation matters, as discussed at length in AT&T's December 18th letter, if the Company were to exclude all such information, along with the other types of information also permitted to be excluded by the Proposals, the required report would contain no substantive information and would mean that the Proposals are inherently impossible to implement.

The Proposals involve AT&T in the political or legislative process.

Mr. Kron's response to AT&T's argument that the Proposals impermissibly involve the Company in the political or legislative process is that they "do not seek an evaluation of a specific legislative process." However, rather than providing a reasoned explanation for his position, Mr. Kron does nothing more than distinguish the no-action precedents cited by AT&T and cite other precedents that can likewise be distinguished from the current Proposals. It is clear from the terms of the Proposals and their Supporting Statements that the Proponents believe that AT&T has participated in government surveillance programs, which the Proponents oppose, and they request management to evaluate the impact that these alleged programs would have on the Company 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.

The Proposals May be Omitted Pursuant to Rules 14a-8(i)(3) and 14a-8(i)(6) Because they are Vague and Indefinite and, As Such, Impossible for AT&T to Implement.

In his objection to AT&T's exclusion of the Proposals 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 Proposals differ from the proposals excluded in the no-action precedents cited by AT&T. In fact, these cases were cited simply to illustrate the Staff's long-held position that the terms of a proposal can be so vague and indefinite 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 Proposals are intrinsically and irreconcilably contradictory. Mr. Kron has failed to point to 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 Proposals are excludable under this standard.

As discussed above, Mr. Kron's arguments as to why the information required by the Proposals is not covered by any of the specific exclusions permitted by the terms of the Proposals are unconvincing. Although Mr. Kron repeatedly attempts to recharacterize the discussion requested by the Proposals as "general," such a discussion would necessarily require AT&T to provide information that is confidential and/or relates to matters of the Company's current litigation and regulatory compliance. Therefore, the Proposals by their own terms, are inherently contradictory - according to the Proposals, AT&T is, at the same time, required to provide information and permitted to exclude the same information. The resolutions' conflicting mandates make the Proposals inherently vague and indefinite and, as such, impossible for AT&T to implement. Mr. Kron's letter does not cite any precedents where inherently contradictory proposals overcame Rule 14a-8(i)(3) and 14a-8(i)(6) arguments and were required to be included in a company's proxy materials.

The Proposals May be Omitted Pursuant to Rule 14a-8(i)(10) Because They Have Been Substantially Implemented.

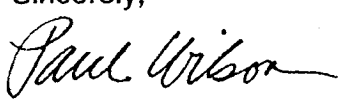
AT&T, insofar as it is able to do so consistent with federal law, has satisfied the substantially implemented standard for excluding the Proposals under

Rule 14a-8(i)(10) because its Privacy Policy already addresses the Proposals' underlying concern. According to Mr. Kron, the Proposals' fundamental goal is "to focus the attention of management on the social policy issue of privacy rights in the context of disclosing customer information without a warrant and the long-term wellbeing of the Company." These are all issues which have been considered by management in developing and implementing the Company's Privacy Policy. While we agree that there are certain differences between AT&T's Privacy Policy and the report required by the Proposals, the Staff's interpretation of Rule 14a-8(i)(10) does not require us to show that AT&T has "fully effected" the Proposals, but only that the Company's actions have satisfactorily addressed the Proposals' underlying concerns. *Exchange Act Release No. 34-20091* (August 16, 1983); *Masco Corp.* (March 29, 1999). AT&T's Privacy Policy satisfies this standard.

* * *

For the reasons set forth above, AT&T continues to believe that it may omit the Proposals from its 2008 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,



Paul Wilson
Senior Attorney

Enclosures

cc: Jonas D. Kron, Attorney at Law

EXHIBIT
1

SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
(202) 736 8010
(202) 736 8711 FAX

BEIJING
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
LONDON

LOS ANGELES
NEW YORK
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

January 17, 2008

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

Re: Shareholder Proposal

Ladies and Gentlemen:

By our letter of December 6, 2007, we provided our legal opinion ("Legal Opinion") that it would violate federal law for AT&T, Inc. to implement a shareholder proposal that has been submitted by Adrian Dominican Sisters and Calvert Asset Management Company, Inc. (the "Proposal") for inclusion in AT&T's next 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 made by Jonas D. Kron, dated January 7, 2008 ("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,

Sidley Austin LLP

Sidley Austin LLP

DWC;dsp

Jonas D. Kron, Attorney at Law

2940 SE Woodward Street
Portland, Oregon 97202
(971) 222-3366 ~ (801) 642-9522
jdkron@kronlaw.com

January 23, 2008

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 2008 Proxy Statement

Dear Sir/Madam:

On behalf of AT&T shareholders Calvert Asset Management Company, Inc., Larry Fahn, and The Adrian Dominican Sisters ("Proponents") this letter is a response to AT&T Incorporated's ("the Company") second letter on this matter, dated January 18, 2008.

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 7th 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.

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. Legal Department Senior Attorney Paul Wilson.

I. The Proponents are Eligible to Submit the Proposal.

Recently, the Staff has addressed the exact same argument that the Company has leveled against Proponent Calvert. In *AT&T Inc.* (January 2, 2008) the Company claimed that documentation provided by State Street for Domini Social Investments was insufficient for the exact same reasons and with respect to the exact same broker (State Street) as in our case. In that context, the Domini Social Investment properly pointed out these assertions are "absurd". We respectfully, request that the Staff come to the same conclusion as in *AT&T* and reject the Company's argument.

With respect to The Adrian Dominican Sisters, we continue to stand by our position that there has not been a violation of Rules 14a-8(b) and 14a-8(f). We would only add that Sister Annette Sinagra of The Adrian Dominican Sisters is fully prepared and able to provide additional proof of ownership as may be required by the Staff.

Finally, with respect to Proponent Larry Fahn we would observe that in 2006 when Mr. Fahn submitted the

2007 proposal, that proposal was addressed to the Chief Executive Officer, AT&T Inc., 175 E. Houston, San Antonio, TX 78205. (Appendix A). That is the identical address that Mr. Fahn sent the Proposal to this year. (Appendix B). In 2006, that address was perfectly acceptable to the Company, but now it is not? Have the Company's mail processing systems significantly degraded in the past year such that it is no longer possible to manage these letters? Mr. Fahn reasonably relied on the fact that the Company accepted the previous shareholder proposal at the CEO's office and should be estopped from asserting such a spurious argument now. Accordingly, we respectfully request that the Staff advise the Company of its view that Mr. Fahn should be viewed as a co-filer.

II. 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 7th letter speak for itself.

However, we would observe that for the third time, **the Company has completely avoided addressing Judge Walker's July 20, 2006 Order** not to mention its present failure to address the supportive reasoning found in the related case *Al-Haramain Islamic Foundation, Inc. v. Bush*, No. 06-36083 (9th Cir. November 16, 2007). Judge Walker's reasoning and conclusions are pivotal to the Staff's decision in the case and the Company's failure to respond at the very least leads one to conclude that it has not met its burden of persuasion. Going further, however, it suggests that the Company has no reasonable argument to rebut Judge Walker's reasoning or conclusions. Therefore, we urge the Staff to reject the Company's arguments in this regard.

III. The Proposal is Focused on Significant Social Policy Issues.

The Company next contends that our arguments "mischaracterize the magnitude of the privacy concerns". The Staff has provided some guidance about what may be considered a significant social policy issue. In Staff Legal Bulletin No. 14A (July 12, 2002) the Staff stated "[t]he Division has noted many times that the ***presence of widespread public debate regarding an issue*** is among the factors to be considered in determining whether proposals concerning that issue 'transcend the day-to-day business matters.'" (emphasis added). Furthermore, the SEC's statement in the 1998 Interpretive Release that a proposal relating to "[ordinary business] matters but focusing on sufficiently significant social policy issues" is not excludable, makes it evident that a subject matter's status as a significant policy issue ***trumps*** the company's portrayal if it as an ordinary business matter. 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. It is only when the Company is able to show that the Proposal raises ***no*** substantial policy consideration that it may exclude the Proposal. 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.

Last week a Mellman Group poll found that "Sixty-three percent of voters favor requiring the government to get a warrant from a court before wiretapping the conversations U.S. citizens have with people in other countries". Furthermore, the poll showed that "**Fifty-seven percent (57%) of voters reject immunity for phone companies** that may have violated the law by selling customers' private information to the

government, preferring to let courts decide the outcome of any cases. Again intensity favors opponents of immunity, with 45% "strongly" opposed." See National Journal's CongressDaily. January 22, 2008. *Reid, McConnell Calls For FISA Action Face Uphill Battle.*

Very recently, the issue of AT&T receiving immunity related to warrantless wiretapping has received heavy Congressional and media attention – and even entering the 2008 Presidential campaigning.

- The New York Times. January 23, 2008. *Democrats Try to Delay Eavesdropping Vote*
- Associated Press. January 23, 2008. *Cheney Wants Surveillance Law Expanded*
- ABC News. December 17, 2007. *Dodd Succeeds in Delaying Wiretapping Bill.*
- Associated Press. December 17, 2007. *Surveillance Bill Delayed Until 2008.*
- Baltimore Sun. December 17, 2007. *Senate punts on FISA bill in face of discord.*
- CBS News. December 17, 2007. *FISA Debate in Senate Delayed Until January.*
- CNNMoney.com. December 17, 2007. *Wiretapping Bill Debate Continues; No Immunity Vote.*
- Detroit Free Press. December 18, 2007. *Security vs. privacy in Senate.*
- The New York Times. December 18, 2007. *Democrats Delay a Vote on Immunity for Wiretaps.*
- Reuters. December 17, 2007. *U.S. Senate postpones consideration of spy bill.*
- San Francisco Chronicle. December 19, 2007. *Feinstein offers compromise: secret court review of wiretap cases.*
- *Washington Post. December 18, 2007. Telecom Immunity Issue Derails Spy Law Overhaul.*

We respectfully disagree with the Company. An issue which polls as this does and receives as much attention as it has in recent weeks by the media (including business media) and senior legislators is a significant policy issue which shareholders have the right to consider.

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.

IV. 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 essence of our analysis is that Judge Walker has concluded that the existence of the Programs and AT&T's participation is not a secret – *points that the Company have not disputed.* 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.

V. AT&T's Privacy Policies for Customers Are Not Substantial Implementation of the Proposal

Because the Proposal Seeks a Discussion of Privacy Rights Issues With Shareholders.

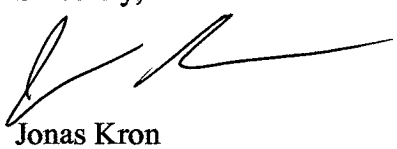
First, the content of the privacy policy clearly does not address the concerns raised by the Proponent. The privacy policy provided by the Company in Company Appendix 8 makes only cursory and conclusory mention of when AT&T would disclose customer information and makes no mention about disclosing communications content. Furthermore, the privacy policy is intended to communicate information to *customers* while the Proposal requests information for *shareholders*. Second, the websites do not present the information in the same form as we request. The Proposal asks for a single report that contains the discussion. While the Company cites to one privacy policy, we observe that there are other privacy policies under the umbrella of AT&T. For example, there is a separate and distinct privacy policy at http://www.wireless.att.com/privacy/. See *Newell Rubbermaid Inc.* (February 21, 2001).

Conclusion

For the reasons given above and in our more extensive letter of January 7, 2008 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 2008 proxy materials.

Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information. Also, pursuant to Staff Legal Bulletin No. 14 B, section F.3. we request the Staff fax a copy of its response to the Proponents at (801) 642-9522.

Sincerely,



Jonas Kron
Attorney at Law
Attorney for the Proponents

Enclosures

cc: Paul Wilson, Senior Attorney, Legal Department, AT&T Inc.

APPENDIX A

As You Sow
Planting Seeds for Social Change
311 California Street, Suite 510
San Francisco, CA 94104
T 415.391.3212
F 415.391.3245
www.asyousow.org

November 6, 2006

Via DHL Express Overnight Mail

Edward E. Whitacre
Chief Executive Officer
A T & T Corporation
175 E. Houston
San Antonio, Texas, 78205

Re: Co-filer Status, 2007 Shareholder Resolution
A T & T – Privacy Rights Protection Report
Primary Filer: Filmmaker Jeremy Kagan, represented by As You Sow

Dear Mr. Whitacre,

As a longtime shareholder of AT&T stock, in my personal account (documentation attached—I have held shares in AT&T for many years, and intend to hold them at least through the 2007 annual meeting of shareholders), I am writing to request that my name be added as a co-filer to the shareholder resolution filed last week by As You Sow, on behalf of primary filer--filmmaker Jeremy Kagan. The proposal is entitled AT&T PRIVACY RIGHTS PROTECTION REPORT. You should be receiving confirmation of other co-filers, including individuals and institutional shareholders over the next few days, prior to the November 11, 2006 filing deadline. I may wish to address management and the Board regarding the Resolution at our annual meeting in the Spring.

I am increasingly concerned about the many reports alleging that our company, AT&T has been complicit in a program whereby we are sharing our customers' private communications data, including e-mail and telephone

communications records, with various entities within the federal government, including the National Security Administration (NSA), the FBI, the CIA and/or others, without first requiring any court order or legal warrant. I feel quite confident that thousands, perhaps hundreds of thousands of my fellow shareholders share that serious concern.

Your silence in response to those reports has been deafening! From everything I can tell, to this day, AT&T has refused to confirm or deny our company's involvement in the alleged NSA warrantless surveillance program, while several of our competitors, including Quest and BellSouth have emphatically denied participation in any such program.

Our company's alleged complicitness, and its subsequent failure to respond to questions about its involvement has caused harm to our built up goodwill and reputation; and has in all likelihood disappointed, discouraged, or even outraged, hundreds or possibly thousands of customers and potential customers, as well as troubled many of our loyal employees and shareholders. In addition the potential legal liabilities (from dozens of lawsuits, including consumer class actions, constitutional violation and infringement cases brought by the American Civil Liberties Union, the Electronic Frontier Foundation and others) are enormous and threaten to undermine the share price that you and everyone else at AT&T have worked so hard to increase.

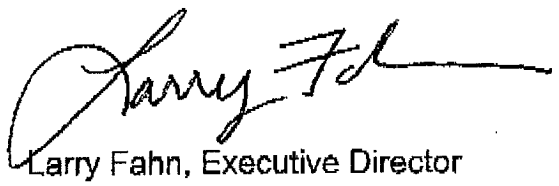
This issue cuts across all ideological and demographic as well as geographic lines. Our right to privacy has long been cherished by folks from all walks of life, conservative, liberal or libertarian, from all parts of the country and across the social spectrum.

AT&T should be leading the charge in promoting the protection of the privacy rights of its customers—not quietly stonewalling efforts of the press, members of Congress or civil liberties groups trying to determine how cooperative our company has been in complying with Administration requests to roll back privacy protections and share sensitive and private communications with branches of our federal government, absent certain protected legal safeguards.

The Privacy Rights Protection Report Resolution should be taken as a corporate governance resolution—we're only asking for transparency, that you file a report explaining the company's position on the privacy rights of its customers, and the ramifications of the company's involvement in the program thus far. You and the Board should give serious consideration to adopting the resolution outright, thus avoiding the attention that might result from having it presented and debated at the Spring '07 annual meeting.

Should you desire to discuss any of the issues raised herein, or in the Resolution, or to begin a dialogue with the stockholders who are filing and co-filing the proposal, feel free to give me, or our corporate social responsibility Program Director Conrad MacKerrron a call at your convenience.

Very Truly Yours,



Larry Fahn, Executive Director
As You Sow

cc: AT&T Board of Directors
As You Sow Board of Directors

APPENDIX B

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

November 20, 2007

Randall L. Stephenson,
Chairman and Chief Executive Officer
AT&T Inc.
175 E. Houston
San Antonio, TX 78205

Re: Shareholder Resolution on Privacy Policy

Dear Mr. Stephenson,

As a shareholder of AT&T, and the Executive Director of As You Sow, I am concerned about reports that AT&T provided customer information to the National Security Agency without a warrant. I 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 shareholders on the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers. It could also have an impact on the share price which may be affected by potential legal liabilities.

Therefore, I am co-filing, with Calvert Asset Management Company and the Adrian Dominican Sisters, the enclosed shareholder proposal for inclusion in the 2008 proxy statement. This filing is in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities Exchange Act of 1934.

I have been an AT&T shareholder continuously for many years and will continue to hold the shares through the 2008 stockholder meeting. I, or my representative, will attend the stockholders' meeting to move the resolution.

Sincerely,

Larry Fahn

Larry Fahn