DC

DIVISION OF
CORPORATION FINANCE

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

February 22, 2007

Mary Louise Weber
Assistant General Counsel
Verizon Communications Inc.
One Verizon Way, Rm VC54S440
Basking Ridge, NJ 07920

Act: 1934
14A-8
a|22|2007

Re: Verizon Communications Inc.
Incoming letter dated December 27, 2006

Dear Ms. Weber:

This is in response to your letters dated December 27, 2006, February 5, 2007 and February 12, 2007 concerning the shareholder proposal submitted to Verizon by Thomas Van Dyck. We also have received letters on the proponent's behalf dated January 23, 2007, February 8, 2007 and February 14, 2007. Our response is attached to the enclosed photocopy of your correspondence. By doing this, we avoid having to recite or summarize the facts set forth in the correspondence. Copies of all of the correspondence also will be provided to the proponent.

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,

David Lynn
Chief Counsel

Enclosures

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

PE

Mary Louise Weber
Assistant General Counsel

One Verizon Way, Rm VC54S440
Basking Ridge, NJ 07920
Phone 908 559-5636
Fax 908 696-2067
mary.l.weber@verizon.com

December 27, 2006

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

Re: Verizon Communications Inc. 2007 Annual Meeting
Shareholder Proposal of Thomas Van Dyck

Ladies and Gentlemen:

This letter is submitted on behalf of Verizon Communications Inc., a Delaware corporation ("Verizon"), pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended. Verizon has received a shareholder proposal and supporting statement (the "Proposal") from Thomas Van Dyck (the "Proponent"), for inclusion in the proxy materials to be distributed by Verizon in connection with its 2007 annual meeting of shareholders (the "2007 proxy materials"). The Proponent has given the organization As You Sow authority to represent him with respect to the Proposal. Copies of the Proposal and all of the correspondence relating to the Proposal are attached as Exhibit A. For the reasons stated below, Verizon intends to omit the Proposal from its 2007 proxy materials.

Pursuant to Rule 14a-8(j)(2), enclosed are six copies of this letter and the accompanying attachments. A copy of this letter is also being sent to As You Sow, on behalf of the Proponent, as notice of Verizon's intent to omit the Proposal from Verizon's 2007 proxy materials.

I. Introduction.

On November 21, 2006, Verizon received a letter from the Proponent containing the following proposal:

RESOLVED: The 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 overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other governmental agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers.

Verizon believes that the Proposal may be properly omitted from its 2007 proxy materials on the following grounds, each of which is discussed in detail below:

- The Proposal may be excluded under Rule 14a-8(i)(7) because it deals with a matter relating to Verizon's ordinary business operations;

- The Proposal may be excluded under Rule 14a-8(i)(2) because, as explained in the opinion of counsel attached to this letter as Exhibit B, implementation of the Proposal would require Verizon to violate one or more federal laws to which Verizon is subject and require Verizon to defy the instructions of the United States Department of Justice;

- The Proposal may be excluded under Rule 14a-8(i)(10) because, to the extent implementation would be consistent with federal law, Verizon has substantially implemented the Proposal; and

- The Proposal may be excluded under Rule 14a-8(i)(3) and 14a-8(i)(6) because the Proposal is so inherently vague and indefinite that neither the shareholders voting on the Proposal nor Verizon in implementing it (if adopted) would be able to determine with any reasonable certainty exactly what measures the Proposal requires.

Verizon respectfully requests the concurrence of the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission (the "Commission") that it will not recommend enforcement action against Verizon if Verizon omits the Proposal in its entirety from its 2007 proxy materials.

II. Bases for Excluding the Proposal.

A. The Proposal May be Excluded Under Rule 14a-8(i)(7) Because it Deals with a Matter Relating to Verizon's Ordinary Business Operations.

Rule 14a-8(i)(7) permits a company to omit a shareholder proposal from its proxy materials if it deals with a matter relating to the company's ordinary business operations. Exchange Act Release No. 34-12999 (November 22, 1976). Where a proposal would require the preparation of a special report to shareholders on specific aspects of the company's business, the Staff "will consider whether the subject matter of the special report involves a matter of ordinary business." Where it does, the proposal will be excludable. Exchange Act Release No. 34-20091 (August 16, 1983).

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." Exchange Act Release No. 34-40018 (May 21, 1998). This general policy reflects two central considerations: (i) "[c]ertain 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) (the "1998 Release"). Verizon believes that these policy considerations clearly justify exclusion of the Proposal. The development and implementation of policies and procedures surrounding the protection of customer information, including the circumstances under which that information may or must be lawfully disclosed, is a basic management function and an integral part of Verizon's day-to-day business operations. Moreover, the proposal addresses matters that are the subject of litigation in which Verizon currently is involved and, consistent with the 1998 Release, a company's litigation strategy is precisely 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 Proposal Impermissibly Seeks to Subject Basic Management Functions --- Protecting Customer Information and Complying With Legal Requirements – to Shareholder Oversight

The Staff has long recognized that proposals which attempt to govern business conduct involving internal operating policies, customer relations and legal compliance programs may be excluded from proxy materials pursuant to Rule 14a-8(i)(7) because they infringe upon management's core function of overseeing business practices. See, e.g., *H&R Block Inc.* (August 1, 2006) (proposal sought implementation of legal compliance program with respect to lending policies); *Bank of America Corporation* (March 3, 2005) (proposal to adopt a "Customer Bill of Rights" and create a position of

"Customer Advocate"); *Deere & Company* (November 30, 2000) (proposal relating to creation of shareholder committee to review customer satisfaction); *CVS Corporation* (February 1, 2000) (proposal sought report on a wide range of corporate programs and policies); *Associates First Capital Corporation* (February 23, 1999) (proposal requested that Board monitor and report on legal compliance of lending practices); *Chrysler Corp.* (February 18, 1998) (proposal requesting that board of directors review and amend Chrysler's code of standards for its international operations and present a report to shareholders); *Citicorp* (January 9, 1998) (proposal sought to initiate a program to monitor and report on compliance with federal law in transactions with foreign entities).

The Staff's no-action letters have expressly found that policies and procedures for protection of customer information are basic customer relations matters. For example, in *Bank of America Corporation* (February 21, 2006), the Staff permitted exclusion of a proposal seeking a report on policies and procedures for protecting customer information. See also *Bank of America Corporation* (March 7, 2005) (same); *Consolidated Edison Inc.* (March 10, 2003) (proposal sought to govern how employees should handle private information obtained in the course of employment); and *Citicorp* (January 8, 1997) (proposal requested report on policies and procedures to monitor illegal transfers through customer accounts).

The development and implementation of policies and procedures for the protection of customer information, including the circumstances under which such information may be lawfully disclosed, is a core management function and an integral part of Verizon's day-to-day business operations. Verizon is one of the nation's largest telecommunications carriers, delivering a wide variety of wireline and wireless communication services to individual consumers, businesses, government and wholesale customers. The level of privacy provided by Verizon to its customers is fundamental to its service offerings and its ability to attract and retain customers. Management is in the best position to determine what policies and procedures are necessary to protect customer privacy and ensure compliance with applicable legal and regulatory requirements. To that end, Verizon has established a Privacy Office which oversees the development and implementation of internal privacy policies and controls that are designed to ensure that customer information is managed in a way that prevents unlawful access or disclosure. The Proposal impermissibly seeks to subject this integral piece of Verizon's business operations to shareholder oversight.

The Proposal Interferes with Verizon's Ability to Respond Effectively to Litigation

Verizon also believes that it may omit the Proposal under Rule 14a-8(i)(7) because the Proposal directly addresses matters that are central to litigation in which Verizon is actively engaged, a fact that the Proposal expressly acknowledges. The Proposal seeks a discussion of Verizon's policies surrounding the alleged disclosure of customer records and communications content to the Federal Bureau of Investigation, NSA and other governmental agencies without a warrant. As disclosed in its Quarterly Reports on Form 10-Q for the second and third quarters of this year, Verizon and a

number of other telecommunications companies have been the subject of multiple class action suits (the "Class Actions") concerning their alleged participation in intelligence-gathering activities allegedly carried out by the federal government, at the direction of the President of the United States, as part of the government's post-September 11 program to prevent terrorist attacks. Plaintiffs generally allege that Verizon has participated by permitting the government to gain access to the content of its subscribers' telephone calls and/or records concerning those calls and that such action violates federal and/or state constitutional and statutory law. The Proposal also seeks a discussion of Verizon's policies surrounding the disclosure of customer records and communications content to non-governmental entities such as private investigators. Verizon's subsidiary, Verizon Wireless, has filed lawsuits against entities and individuals who pose as customers or employees, a practice known as "pre-texting," to unlawfully access phone records of Verizon Wireless subscribers; one of these lawsuits arises out of the pretexting associated with the investigation by the Hewlett-Packard Company into leaks of confidential information from its Board of Directors.

The Staff has permitted the exclusion under Rule 14a-8(i)(7) of shareholder proposals that could interfere with the company's ability to respond effectively to litigation and governmental investigations. See, e.g., *Reynolds American Inc.* (February 10, 2006) (proposal requesting that the company conduct a campaign to apprise African Americans of health hazards associated with menthol cigarettes was excludable where the company was defending lawsuits relating to same matter); *Loews Corporation* (March 22, 2006) (same); *R. J. Reynolds Tobacco Holding Inc.* (February 6, 2004) (proposal requesting that the company refrain from marketing cigarettes as "light" until independent research shows light brands actually reduce health risks was excludable because it interfered with litigation strategy of a class action lawsuit on similar matters); and *R. J. Reynolds Tobacco Holding Inc.* (March 6, 2003) (proposal seeking a report assessing the company's involvement in international cigarette smuggling was properly excludable under Rule 14a-8(i)(7) where the company was defending lawsuits relating to the same matter).

Even if the Proposal is deemed to touch upon significant policy issues, under these precedents a shareholder proposal is nevertheless excludable if it implicates litigation strategy. For example, in *Philip Morris Companies, Inc.* (February 4, 1997), the Staff noted that it previously had "taken the position that proposals directed at the manufacture and distribution of tobacco-related products by companies involved in making such products raise issues of significance that do not constitute matters of ordinary business," but nevertheless determined that the company could exclude " a proposal [that] primarily addresses the litigation strategy of [the company], which is viewed as inherently the ordinary business of management to address." This result is also consistent with the longstanding position of the Staff that a company's decision to institute or defend itself against legal actions, and decisions on how it will conduct those legal actions, are matters relating to ordinary business operations within the exclusive prerogative of management. See, e.g., *NetCurrents, Inc.* (May 8, 2001) (proposal requiring company to sue two individuals within 30 days of annual meeting excludable

as ordinary business operations because it relates to litigation strategy); and *Microsoft Corporation* (September 15, 2000) (proposal asking company to sue federal government on behalf of shareholders excludable as ordinary business because it relates to the conduct of litigation).

The Proposal squarely implicates issues that are central to both the Class Actions and the Verizon Wireless lawsuits. To comply with the request of the Proposal, or even take a public position on the subject matter of the Proposal in its 2007 proxy materials, would improperly interfere with and otherwise adversely affect Verizon's litigation strategy in the Class Actions. In addition, as discussed in further detail below, Verizon has been furnished with an opinion of counsel that implementing the Proposal would require Verizon to violate one or more federal laws and defy the instructions of the United States Department of Justice concerning the treatment of classified information which Verizon may possess. As such, inclusion of the Proposal in Verizon's 2007 proxy materials would permit Proponent to interfere with management's right and duty to determine Verizon's litigation strategy.

The Proposal Inappropriately Seeks to Engage Verizon in Political Discourse Implicating Verizon's Ordinary Business Operations.

The Staff consistently has permitted a proposal to be excluded under Rule 14a-8(i)(7) where the proposal appeared to be directed at engaging the company in a political or legislative process relating to an aspect of its business operations. See, e.g., *Microsoft Corporation* (September 29, 2006) (permitting exclusion of proposal seeking report on the company's rationale for supporting certain public policy measures concerning regulation of the internet); *Verizon Communications Inc.* (January 31, 2006) (permitting exclusion of proposal seeking report on the impact of flat tax); *International Business Machines Corporation* (March 2, 2000) (proposal seeking establishment of a board committee to evaluate the impact of pension-related proposals under consideration by national policymakers was excludable). See also *Pacific Enterprises* (February 12, 1996) (proposal that a utility dedicate its resources to ending state utility deregulation was excludable); *Pepsico, Inc.* (March 7, 1991) (permitting exclusion of proposal calling for an evaluation of the impact on the company of various federal healthcare proposals); *Dole Food Company* (February 10, 1992) (same); and *GTE Corporation* (February 10, 1992) (same).

In *International Business Machines, supra,* the Staff's letter allowing exclusion of the proposal specifically noted that "the proposal appears directed at involving IBM in the political or legislative process relating to an aspect of IBM's operations." Here, the Proponent clearly wants to commandeer the resources of Verizon and the platform of its proxy statement to criticize measures allegedly taken by the federal government, at the direction of the President of the United States, as part of the government's post-September 11 program to prevent terrorist attacks. The Proposal suggests that Verizon has been complicit in violations of customer privacy, including the practice of pre-texting, and asserts, "[t]hese issues pose questions in regard to general respect for the

rule of law upon which our democratic system depends." On a day-to-day basis Verizon devotes substantial resources to monitoring compliance with laws relating its handling of customer information, cooperating with lawful requests for information from law enforcement agencies and others and actively participating in ongoing regulatory, legislative and judicial proceedings relating to privacy issues. The Proposal inappropriately seeks to intervene in Verizon's routine management of this basic area of its business in order to advance a specific political or legislative objective.

The fact that a proposal may touch upon a matter with public policy implications does not necessarily remove it from the realm of ordinary business matters. Rather, no action precedents demonstrate that the applicability of Rule 14a(i)(7) depends largely on whether implementing the proposal would have broad public policy impacts outside the company or would only deal with matters of the company's internal business operations, planning and strategy. For example, in *Microsoft Corporation, supra,* the Staff permitted exclusion of a proposal relating to a significant policy issue (i.e., net neutrality), because it recognized that evaluating the impact of expanded government regulation of the internet was a matter of the company's internal business operations, planning and strategy. Implementing the Proposal would involve matters central to Verizon's internal business operations, planning and strategy; namely, analysis of the myriad issues that arise in connection with, and the attendant risks of, safeguarding private customer information and complying with applicable legal and regulatory requirements.

For all of the foregoing reasons, Verizon believes that the Proposal may be omitted from its 2007 proxy materials because it deals with matters relating to Verizon's ordinary business operations.

B. The Proposal May Be Omitted Under Rule 14a-8(i)(2), Because Implementation of the Proposal Would Require Verizon to Violate One or More Federal Laws and Defy the Instructions of the United States Department of Justice Concerning the Treatment of Classified Information.

A shareholder proposal may be properly excluded under Rule 14a-8(i)(2) if the proposal, if implemented, would cause the company to violate any state, federal or foreign law to which it is subject. Verizon has been furnished with an opinion of counsel that implementation of the Proposal's central request – namely, that Verizon report on the legal and other policy issues surrounding the disclosure of customer information to federal agencies without a warrant -- would be a violation of one or more federal laws to which Verizon is subject and would defy the instructions of the United States Department of Justice. As more fully explained in the opinion of counsel, which is attached to this letter as Exhibit B, the United States has expressly and formally advised Verizon on several occasions that it would violate federal law if it were to disclose classified information it may possess concerning intelligence-gathering activities allegedly carried out by the federal government, at the direction of the

President of the United States, as part of the government's post-September 11 program to prevent terrorist attacks. These issues are discussed in detail in the accompanying opinion of counsel, and are incorporated into this letter.

Even though implementation of the Proposal's secondary request – namely, that Verizon report on the legal and other policy issues surrounding the disclosure of customer information in the context of "pretexting" –would not result in a violation of law, Verizon believes that it may nevertheless exclude the Proposal under Rule 14a-8(i)(2). In Staff Legal Bulletin No. 14 (July 13, 2001), the Staff made it clear that it will only permit shareholders to revise their proposals and supporting statements in limited circumstances, stating, "when a proposal and supporting statement will require detailed and extensive editing in order to bring them into compliance with the proxy rules, we may find it appropriate for companies to exclude the entire proposal, supporting statement, or both, as materially misleading." (Staff Response to Question E. 1). Here, detailed and extensive editing would be required in order to bring the Proposal into compliance with the proxy rules, namely Rule 14a-8(i)(2). Not only would the first clause of the Resolution need to be deleted in its entirety, but also significant portions of the lengthy preamble would require detailed revision. In the eight paragraph preamble, the third, fourth and fifth paragraphs would have to be deleted in their entirety, and substantial modifications would be necessary in the sixth and eighth paragraphs. In addition, in Staff Legal Bulletin No. 14 the Staff provided the following example of the limited type of change it may consider permissible under Rule 14a-8(i)(2): "If implementing the proposal would require the company to breach existing contractual obligations, we may permit the shareholder to revise the proposal so that it applies only to the company's future obligations." (Staff Response to Question E.5) In contrast to this example, the defect of the Proposal could not be easily cured by making a minor revision. Finally, there is no-action precedent under Rule 14a-8(i)(7) to support the exclusion of a proposal in its entirety where only part of the proposal relates to ordinary business matters. See *CVS Corporation* (February 1, 2000) (permitting exclusion of a proposal requesting a strategic report where some of the requested topics were ordinary business matters); and *Chrysler Corporation* (March 18, 1998) (permitting exclusion of proposal requesting review and report on code of standards for foreign operations). Verizon believes that the analysis applied in the context of Rule 14a-8(i)(7) is equally applicable to Rule 14a-8(i)(2).

Verizon believes that the Proposal may be omitted from its 2007 proxy materials because implementation of the central request of the Proposal would violate one or more federal laws to which Verizon is subject and would defy the instructions of the United States Department of Justice. Permitting significant revision and restatement of the balance of the Proposal would be inconsistent with the Staff's stated position and numerous precedent.

C. The Proposal May Be Excluded Under Rule 14a-8(i)(10), Because Verizon Has Substantially Implemented the Proposal.

Verizon also believes that it may exclude the Proposal under Rule 14a-8(i)(10) because, to the extent the Proposal may be read as seeking information describing the issues surrounding the disclosure of customer information to third parties and customer privacy rights, Verizon has already substantially implemented the request insofar as it is able to do so consistent with federal law. Verizon has posted extensive materials addressing these issues on its various websites as noted below.

The "substantially implemented" standard reflects the Staff's interpretation of the predecessor rule (allowing omission of a proposal that was "moot") that a proposal need not be "fully effected" by the company to meet the mootness test so long as it was "substantially implemented." See SEC Release No. 34-20091 (August 16, 1983). Pursuant to the 1983 interpretation, the Staff has stated that "a determination that the company has substantially implemented the proposal depends upon whether its particular policies, practices and procedures compare favorably with the guidelines of the proposal." *Texaco, Inc.* (March 28, 1991). See, also, *Nordstrom Inc.* (February 8, 1995 (proposal that company commit to code of conduct for overseas suppliers that was substantially covered by existing company guidelines) and *The Gap, Inc.* (March 8, 1996) (same). Other Staff no-action letters have established that a company need not comply with every detail of a proposal in order to exclude it under Rule 14a-8(i)(10). Differences between a company's actions and a proposal are permitted so long as a company's actions satisfactorily address the proposal's underlying concerns. See *Masco Corporation* (March 29, 1999) (permitting exclusion because the company adopted a version of the proposal with slight modification and a clarification as to one of its terms). In addition, proposals have been considered "substantially implemented" where the company has implemented part but not all of a multi-faceted proposal. See *Columbia/HCA Healthcare Corp.* (February 18, 1998) (permitting exclusion of proposal after company took steps to partially implement three of four actions requested by the proposal).

The home page of Verizon's internet website (www.verizon.com) contains a link entitled "Privacy Policy." That link brings the reader to Verizon's "Privacy and Customer Security Policies." Through additional links, readers may access numerous pages explaining Verizon's policy and procedures with respect to telephone company customer privacy and internet privacy, as well as Verizon's general privacy principles. The principles govern all aspects of how individual customer information is handled across Verizon's businesses, including how it is collected and used, how customers are informed of their rights, when and to whom it may be disclosed and how Verizon implements its privacy practices.

Likewise, the home page of Verizon Wireless' internet website (www.verizonwireless.com) contains a link entitled "Privacy Policy" and the home page of

Verizon Online's internet website (www.verizononline.net) contains a link entitled "Verizon Online Privacy Statement", each of which provides access to materials explaining the company's policies and procedures with respect to customer privacy. All of the Verizon companies' websites contain links to Verizon's general privacy principles.

Verizon believes that all of these publicly available materials, taken together, substantially implement the Proposal's request for information describing the issues surrounding the disclosure of customer information and the impact of that disclosure on the privacy rights of Verizon customers, to the extent consistent with federal law. Because the materials clearly address the underlying concern expressed by the Proposal, Verizon is of the view that the Proposal may be properly omitted from its 2007 proxy materials pursuant to Rule 14a-8(i)(10).

D. The Proposal May Be Omitted Under Rule 14a-8(i)(3) and Rule 14a-8(i)(6), Because It is Inherently Vague and Indefinite

Notwithstanding the fact that Verizon believes that Verizon's publicly available materials substantially implement, to the extent consistent with federal law, the request of the Proposal under Rule 14a-8(i)(10), Verizon also believes that the Proposal may be properly excluded under Rule 14a-8(i)(3) and Rule 14a-8(i)(6), because the Proposal's description of the requested report is so vague and indefinite 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).

Rule 14a-8(i)(3) permits a company to omit a shareholder proposal and the related supporting statement from its proxy materials if such "proposal or supporting statement is contrary to any of the Commission's proxy rules, including [Rule] 14a-9, which prohibits materially false or misleading statements in proxy soliciting materials." According to the Staff, a proposal will violate Rule 14a-8(i)(3) when "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 exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (September 15, 2004). See, also, *FirstEnergy Corp.* (February 18, 2004) (permitting exclusion of proposal urging Board to change company's governing documents relating to shareholder approval of shareholder proposals, because requested vote requirement was vague and misleading); *Global Entertainment Holdings/Equities, Inc.* (July 10, 2003) (permitting omission of a proposal that Board adopt an "action plan" which "accounts" for past sale of a business and resulting licensing arrangements, because it was vague and indefinite); *Pfizer Inc.* (February 18, 2003) (supporting omission of a proposal requesting board make all stock options at no less than the "highest stock price" and that the stock options contain a buyback provision, because action requested was vague and indefinite); *Johnson & Johnson* (February 7, 2003) (permitting omission of a shareholder proposal that called for a report on the company's "progress with the

Glass Ceiling Report", but did not explain the substance of the report); *H.J. Heinz Co.* (May 25, 2001) (supporting the omission of a shareholder proposal under Rule 14a-8(i)(3) where the proposal requested the company to implement the SA8000 Social Accountability Standards, but did not clearly set forth what SA8000 required of the company); *Kohl's Corp.* (March 13, 2001) (same); and *Philadelphia Electric Co.* (July 30, 1992) (supporting the omission of a shareholder proposal under predecessor Rule 14a-8(c)(3) where a proposal resolved that a committee of small stockholders would refer a "plan or plans" to the board, but did not describe the substance of those plans). In addition, a company may exclude a shareholder proposal under Rule 14a-8(i)(6) if it is beyond the company's power to implement it. A company lacks the power or authority to implement a proposal under Rule 14a-8(i)(6) when the proposal in question "is so vague and indefinite that [the company] would be unable to determine what action should be taken." *International Business Machines Corporation* (January 14, 1992).

Like these proposals, the Proposal may be properly excluded from Verizon's 2007 proxy materials because it is so vague and indefinite that it is open to a myriad of interpretations and would be impossible for either the shareholders or the Verizon Board to ascertain precisely what implementation of the proposal would entail. For example:

- The tenor and tone of the lengthy Whereas clause clearly emphasize that the Proposal seeks an explanation of whether Verizon disclosed customer records and communications content to one or more federal agencies without a warrant and to unauthorized private individuals;

- The Proposal requires the report be drafted "excluding confidential and proprietary information," while failing to define that term. To the extent the Proposal means to exclude any classified information from the report, the result would be an entirely abstract study, as discussed immediately below. To the extent the Proposal means only to exclude information proprietary to Verizon, the Proposal would require Verizon to violate federal law as discussed above.

- The Resolution calls for an abstract "overarching" discussion of the "technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content" to governmental agencies without a warrant or to private individuals , as well as the effect of any such disclosure on the privacy rights of customers. The "overarching" discussion which the Resolution contemplates be included in the report is vague and indefinite, and is more suited to a graduate student's doctoral thesis or a government "white paper" than to a corporate report to shareholders.

- The Whereas clause refers to the "potentially negative uses of today's technology" as a reason that Verizon should undertake the requested report, but it is unclear what is meant by this or by the Resolution's reference to "technological policy issues" surrounding the disclosure of customer information.

- The Whereas clause seems to acknowledge Verizon's well-publicized policy against the practice known as pretexting and its efforts to bar the practice by other entities, but at the same time also insinuates that Verizon is somehow responsible for the fact that pre-texting was used to obtain phone records in connection with the Hewlett-Packard Company's investigation.

In numerous instances, the Staff has permitted the exclusion of a proposal requesting a report where the proposal contains only general or uninformative references to the complex or multifaceted set of issues implicated by the proposal. See, for example, *The Ryland Group, Inc.* (January 19, 2005); *Kroger, Co.* (March 19, 2004); *Albertsons, Inc.* (March 5, 2004); and *Terex Corp.* (March 1, 2004), where, in each case, the Staff permitted exclusion of a proposal requesting a report based on the Global Reporting Initiative's sustainability guidelines. Like these proposals, the Proposal should be excludable because it is so vague and indefinite that it would be impossible for either the shareholders or the Verizon Board to ascertain precisely what implementation of the proposal would entail.

III. Conclusion.

Verizon believes that the Proposal may be omitted from its 2007 proxy materials (1) under Rule 14a-8(i)(7) because it deals with matters relating to Verizon's ordinary business operations, (2) under Rule 14a-8(i)(2) because implementation of the proposal would result in a violation of law, (3) under Rule 14a-8(i)(10) because, to the extent consistent with law, Verizon has already substantially implemented the Proposal, and (4) under Rule 14a-8(i)(3) and 14a-9 because the Proposal is vague and indefinite. Accordingly, Verizon respectfully requests the concurrence of the Staff that it will not recommend enforcement action against Verizon if Verizon omits the Proposal in its entirety from Verizon's 2007 proxy materials.

Verizon requests that the Staff fax a copy of its determination of this matter to the undersigned at (908) 696-2068 and to the representative of the Proponent at (415) 391-3245.

Kindly acknowledge receipt of this letter by stamping and returning the extra enclosed copy of this letter in the enclosed self-addressed, stamped envelope. If you have any questions with respect to this matter, please telephone me at (908) 559-5636.

Very truly yours,

Mary Louise Weber

Mary Louise Weber
Assistant General Counsel

Enclosures
cc: As You Sow
311 California Street, Suite 510
San Francisco, CA 94104

EXHIBIT "A"

As You Sow

A Foundation Planting Seeds for Social Change

311 California St., Suite 510, San Francisco, CA 94104 — Phone (415) 391-3212 — Fax (415) 391-3245

Facsimile Cover Sheet

Date **11-29-06**

To/Fax **Marianne Drost**
Corporate Secretary
Verizon

From **Conrad MacKerron**

Total pages being transmitted, including cover page 2

Dear Ms Drost:

Attached please find a corrected copy of my letter filing a shareholder proposal with the company.

Thank you.

Conrad MacKerron

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

Nov. 20, 2006

Marianne Drost
Corporate Secretary
Verizon Communications
140 West Street, 29th Floor
New York, NY 10007

By overnight mail and fax 908-766-3813

Dear Ms. Drost:

As You Sow is a non-profit organization whose mission is to promote corporate accountability. We represent Mr. Thomas Van Dyck, a shareholder of Verizon stock.

We are concerned about reports that Verizon's MCI long-distance division may have provided customer information to the National Security Agency without a warrant. We believe this action may have compromised customer privacy protections and presents the potential for increased legal liability for the company. Further, it could affect Verizon's reputation and good standing. This alleged program has resulted in numerous press stories on the subject and the filing of lawsuits against the company. It is important for the company to report to stockholders on legal and ethical issues surrounding disclosure of the content of customer communications to federal authorities without a warrant, as well as the impact this action may have on our customers.

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

Proof of ownership and authorization to act for Mr. Van Dyck is attached. The shareholder will continue to hold the shares through the 2007 stockholder meeting. A representative of the filer will attend the stockholders' meeting to move the resolution.

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

Sincerely,

Conrad B. MacKerron
Director, Corporate Social Responsibility Program

Enclosures

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

Nov. 20, 2006

Marianne Drost
Corporate Secretary
Verizon Communications
140 West Street, 29th Floor
New York, NY 10007

By overnight mail and fax 908-766-3813

Dear Ms. Drost:

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

We are concerned about reports that Verizon's MCI long-distance division may have provided customer information to the National Security Agency without a warrant. We believe this action may have compromised customer privacy protections and presents the potential for increased legal liability for the company. Further, it could affect Verizon's reputation and good standing. This alleged program has resulted in numerous press stories on the subject and the filing of lawsuits against the company. It is important for the company to report to stockholders on legal and ethical issues surrounding disclosure of the content of customer communications to federal authorities without a warrant, as well as the impact this action may have on our customers.

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

Proof of ownership and authorization to act for Mr. Van Dyck is attached. The shareholder will continue to hold the shares through the 2007 stockholder meeting. A representative of the filer will attend the stockholders' meeting to move the resolution.

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

Sincerely,

Conrad B. MacKerron
Director, Corporate Social Responsibility Program

Enclosures

VERIZON -- PRIVACY RIGHTS PROTECTION REPORT

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

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

The reputation and good standing of Verizon may be placed in jeopardy by reports that its subsidiary MCI may have voluntarily provided customer phone records and communications data to the National Security Agency (NSA); and

We believe this alleged practice is seen by millions of Americans, including customers, shareholders and employees of Verizon, as a violation of our customers' privacy expectations and basic right to have phone and e-mail records kept confidential; and

Verizon management has not confirmed or denied reports that its long-distance carrier MCI released consumer data to the NSA. Multiple class action and other consumer lawsuits have been filed against Verizon which could result in millions of dollars in liabilities and defense fees; and

Our customers have the choice to go to other telecommunications companies if they do not agree with the company's practices and may do so. These events and the potential for legal liability could affect the long-term value of our company; and

We are also concerned about ongoing violations of customer privacy including pretexting. This practice was used by Hewlett-Packard management to obtain data on phone calls made by board members. Verizon President Lawrence Babbio is an HP board member. Shareholders deserve an explanation of how pretexting could have occurred under Mr. Babbio's watch on the HP board. We believe Verizon executives are fully aware of the illegality of pretexting as demonstrated by the Verizon Wireless lawsuit filed against the individuals who obtained its customers' cell phone records as part of the HP investigation; and

These issues pose questions in regard to general respect for the rule of law upon which our democratic system depends. In light of the potentially negative uses of today's technology, we believe it is important that Verizon re-examine the steps it takes to protect the values embodied in an individual's right to privacy.

RESOLVED: The 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 overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other government agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers.

SUPPORTING STATEMENT

We believe it will benefit society, our customers, shareholders and Verizon's long-term value for the company to take a leadership role as protector of privacy rights and to issue this report. The proponents urge a YES vote.

Nov. 20, 2006

Conrad MacKerron
Director, Corporate Social Responsibility Program
As You Sow Foundation
311 California St., Ste. 510
San Francisco, CA 94104

Dear Mr. MacKerron:

I authorize As You Sow to file a shareholder resolution on my behalf at Verizon.

The resolution asks the company to issue a report that describes issues, policies and procedures concerning the integrity of customer privacy rights and confidentiality of customer information.

I am the owner of more than $2000 worth of Verizon stock that has been held continuously for more than one year and will be held through the date of the company's next annual meeting.

I give As You Sow full authority to deal, on my behalf, with any and all aspects of this shareholder resolution. I understand my name may appear on the company's proxy statement as filer of the aforementioned resolution.

Sincerely,

Thomas Van Dyck

RBC
Dain Rauscher

SRI Wealth Management Group
345 California Street
29th Floor
San Francisco, CA 94104
(415) 445-8306
(415) 445-8313 Fax
(866) 408-2667 Toll Free

To Whom It May Concern:

This is to confirm that Thomas Van Dyck is the beneficial owner of at least $2000 worth of Verizon stock, and that those shares have been held continuously for at least one year and will be held through the date of the company's next annual meeting.

Sincerely,

11/20/06

Taman Rapp

WILMERHALE

December 27, 2006

Board of Directors
Verizon Communications Inc.
c/o Mr. William P. Barr, General Counsel
One Verizon Way, Fourth Floor
Basking Ridge, New Jersey 07920

Re: Shareholder Proposal

Dear Members of the Board:

We have acted as special counsel to Verizon Communications Inc. ("Verizon") in litigation and related proceedings concerning Verizon's alleged involvement in certain intelligence-gathering activities of the federal government. In connection with that representation, you have requested our legal opinion as to whether it would violate federal law for Verizon to implement a shareholder proposal submitted by Mr. Thomas Van Dyck (the "Proposal") to Verizon for inclusion in its 2007 proxy statement.

Our opinion is limited to the specific issues addressed in this Letter and is further limited in all respects, except as otherwise stated, to the facts assumed and laws existing on the date of this Letter. By rendering our opinion, we do not undertake to advise you of any changes in the laws or facts that may occur after the date of this Letter.

Consistent with your request, we express an opinion only with respect to the federal laws of the United States of America. We express no opinion as to the applicability of the law of any state or any other jurisdiction.

THE PROPOSAL

The Proposal was submitted on Mr. Van Dyck's behalf by Mr. Conrad B. MacKerron of As You Sow, a nonprofit organization. In forwarding the Proposal, Mr. MacKerron expressed "concern[] about reports that Verizon's MCI long-distance division may have provided customer information to the National Security Agency without a warrant." Mr. MacKerron's letter states that "[t]his alleged program has resulted in numerous press stories on the subject and the filing of lawsuits against the company."

The Proposal requests, in light of media reports and pending litigation, "that the Board of Directors issue a report to shareholders, at reasonable cost and excluding confidential and proprietary information," that "describes the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications contents to (1) the Federal Bureau of Investigation, NSA [National Security Agency] and other government

agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers."[1]

The media reports and litigation on which the Proposal is premised relate to two alleged counterterrorism programs. First, in December 2005, *The New York Times* reported that the NSA has intercepted the telephone communications of persons in the United States with persons located abroad whom the NSA reasonably suspects are members of al Qaeda or of organizations affiliated with al Qaeda.[2] In response to that report, the President acknowledged the existence of a contents-interception program—called the Terrorist Surveillance Program ("TSP")—and the Attorney General issued a written explanation of the legal authorities supporting the TSP.[3]

The second alleged program relates not to the contents of communications, but rather to the call records of telecommunications customers. *USA Today* reported in May 2006 that, after September 11, 2001, the NSA gathered customer call records from major telecommunications carriers and analyzed the records for calling patterns that might help to identify terrorist activity.[4] The government has not publicly confirmed or denied whether the alleged call-records program exists or, if it does, whether any particular telecommunications carrier has participated. We will refer collectively to the TSP and alleged call-records program as the "Alleged Programs."

Nothing in this Letter should be construed as an admission or denial of Verizon's involvement in the Alleged Programs. For the purpose only of responding to your request, we accept at face value the facts asserted in the media reports. No inference regarding the truth of the reports can be drawn from these assumptions, nor should anything in this Letter be construed as an admission or denial of Verizon's involvement in the Alleged Programs.

---

1 Our Letter does not address the second of these two topics (*i.e.*, the alleged disclosure of customer information to non-governmental entities).

2 *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

3 *See* U.S. Dep't of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006).

4 *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, at 1A. *USA Today* has since partially retracted its account and reported that it "cannot confirm that BellSouth or Verizon contracted with the NSA to provide bulk calling records to [the NSA] database." *See A Note to Our Readers*, USA Today, June 30, 2006, *available at* http://www.usatoday.com/news/washington/2006-06-30-nsa_x.htm.

ANALYSIS

The Proposal seeks a Board report that would "exclud[e] confidential and proprietary information." Although the Proposal does not define the phrase "confidential and proprietary information," there are two possible understandings of that phrase in this context: (1) information that the United States government has designated as classified, or (2) internal proprietary information of Verizon, such as that typically subject to intellectual property and trade secrets protections.

For purposes of this Letter, we assume that the Proposal means to exclude "confidential and proprietary information" in the second meaning of the term only—intellectual property secrets and the like.[5] Accordingly, we further assume that the Proposal does not exclude government-classified information or materials from the proposed Board report. As we explain below, federal law prohibits Verizon from disclosing classified information, if any, in its possession.

1. *The United States Has Informed Verizon That Information Pertaining to the Alleged Programs Is Classified.*

In various lawsuits concerning the Alleged Programs, the United States has invoked the state-secrets privilege. That privilege is a common law evidentiary doctrine that allows the government to deny access in litigation to classified information where a reasonable danger exists that revealing the information in court proceedings would harm national security interests, impair national defense capabilities, disclose intelligence-gathering methods or capabilities, or disrupt diplomatic relations with foreign governments.[6] The government may invoke the privilege to withhold a broad range of information; and once the court determines that further proceedings would divulge state secrets, the privilege is absolute.[7] In invoking the state-secrets

---

[5] If the Proposal means to exclude "confidential and proprietary information" in the first sense—that is, materials classified by the government—then it seeks only an advisory report on "the overarching technological, legal and ethical policy issues surrounding disclosure of customer records and communications content" to certain entities. We do not express an opinion on whether this is the intended meaning of the Proposal, nor does this Letter address this possible interpretation.

[6] *See United States v. Reynolds*, 345 U.S. 1, 7-11 (1953).

[7] *See, e.g., Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

privilege in litigation pertaining to the Alleged Programs, the United States has asserted that the classified nature of the government's intelligence efforts bars the litigation from proceeding.[8]

The United States has stated that any information relating to the TSP beyond what the government has publicly confirmed—and information, if any, concerning the alleged call-records program, which the government has neither confirmed nor denied—is classified. The Attorney General has explained that the TSP is "probably the most classified program that exists in the United States government."[9] The Director of National Intelligence, through sworn affidavits asserting the state-secrets privilege in litigation, has formally identified information concerning the Alleged Programs as classified. In a related case pending against AT&T, Director Negroponte has specifically declared that the state-secrets privilege precludes disclosure of "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." Unclassified Declaration of the Honorable John D. Negroponte ¶ 11. The United States has indicated that it will make the same state-secrets assertion with respect to the cases pending against Verizon.[10]

The courts have ratified the government's assertion that information related to the Alleged Programs may not be disclosed. Two courts have dismissed claims concerning the alleged call-records program as barred by the state-secrets privilege.[11] In a third case, *Hepting*, 439 F. Supp. 2d at 997-998, the district court recognized that the state-secrets privilege prevents claims pertaining to the alleged call-records program from proceeding, though it did not dismiss the claims at the threshold. With respect to the TSP, the *Hepting* court denied the United States' motion to dismiss on state-secrets grounds but acknowledged that the privilege bars the disclosure of some information concerning the Program. *Id.* at 994-995. And finally, another

---

8 *See ACLU v. NSA*, 438 F. Supp. 2d 754, 758-59 (E.D. Mich. 2006); *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 900 (N.D. Ill. 2006); *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 979 (N.D. Cal. 2006).

9 Press Conference of Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2006), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

10 Notice of Motion and Motion To Intervene by the United States of America, *Riordan v. Verizon Communications Inc.*, No. 06-3574-VRW (N.D. Cal. Aug. 4, 2006).

11 *See ACLU v. NSA*, 438 F. Supp. 2d at 765; *Terkel*, 441 F. Supp. 2d at 917.

court recently held that a federal statute and Executive Order protect information about the TSP from disclosure under the Freedom of Information Act.[12]

To the extent the Proposal is properly understood as requesting or requiring the disclosure of classified information pertaining to the Alleged Programs, if any, in Verizon's possession, the United States has advised Verizon that such disclosure is prohibited.

2. *Federal Law Prohibits Unauthorized Disclosure of Classified Information.*

The United States has expressly instructed Verizon that disclosing any classified information Verizon might possess concerning the Alleged Programs would violate federal law. The United States has also filed federal court actions to prevent Verizon from responding to subpoenas by various state officials requesting information about any involvement Verizon may have had in the Alleged Programs.[13]

In a letter directed to us in our capacity as Verizon's counsel, the United States Department of Justice advised that responding to subpoenas seeking information about the Alleged Programs—"including by disclosing whether or to what extent any responsive materials exist—would violate federal laws and Executive Orders."[14] In a related letter to the Attorney General of New Jersey concerning subpoenas she issued to Verizon and other telecommunications carriers regarding the Alleged Programs, the Department of Justice identified several federal statutes and Executive Orders that it said a response by the carriers to the subpoenas would violate.[15]

First, it is a federal crime knowingly and willfully to divulge specified categories of classified information to any unauthorized person. In particular, 18 U.S.C. § 798(a) provides:

---

[12] *People for the Am. Way Found. v. NSA/CIA*, No. 06-206, 2006 WL 3359589, at *7-*8 (D.D.C. Nov. 20, 2006).

[13] *See, e.g., United States v. Rabner*, No. 3:06-cv-02683-FLW-TJB (D.N.J.); *United States v. Volz*, No. 2:06-cv-188 (D. Vt.).

[14] Letter from Assistant Attorney General Peter D. Keisler to John A Rogovin *et al.*, June 14, 2006, at 1.

[15] Letter from Assistant Attorney General Peter D. Keisler to the Honorable Zulima V. Farber, Attorney General of New Jersey, June 14, 2006, at 3-4.

> 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. 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." *Id.* § 798(b). The statute defines "communication intelligence" as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." *Id.*

Other federal laws also protect the confidentiality of classified information and prohibit its disclosure. 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 on the Director of National Intelligence the authority to "protect intelligence sources and methods from unauthorized disclosure." *Id.*[16] Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 65, codified at 50 U.S.C. § 402 note, 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 persons employed by such agency." *Id.*[17]

The Federal Bureau of Investigation ("FBI") is also authorized to obtain customer information from telecommunications carriers upon application for a Foreign Intelligence Surveillance Act ("FISA") court order without a conventional warrant, and the statute prohibits the carrier, subject to certain exceptions not applicable here, 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."[18] The Stored Communications Act also authorizes the FBI to obtain transactional, billing, or calling records from a wire or electronic communication service provider without a court order in certain situations implicating national security, and the provision bars the carrier from disclosing that it received or fulfilled such a request (subject to exceptions not applicable here).[19]

Several Executive Orders also restrict the disclosure of national security information. Executive Order No. 12958, 60 Fed. Reg. 19,825 (Apr. 17, 1995), as amended by Executive Order No. 13,292, 68 Fed. Reg. 15315 (Mar. 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."[20]

---

16 The Supreme Court has recognized the Executive's authority to protect intelligence sources and methods. *See CIA v. Sims*, 471 U.S. 159, 169 (1985); *Snepp v. United States*, 444 U.S. 507, 509 (1980).

17 *See also Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996) ("The protection afforded by section 6 is, by its very terms, absolute."); *Founding Church of Scientology v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Hayden v. NSA*, 608 F.2d 1381, 1390) (D.C. Cir. 1979).

18 50 U.S.C. § 1861(d).

19 18 U.S.C. § 2709(c).

20 Exec. Order No. 13292 § 4.1(a), (c).

This broad array of federal laws and Executive Orders does not permit a company to disclose without authorization any classified information it might possess. Accordingly, to the extent the Proposal requires Verizon to reveal classified information pertaining to the Alleged Programs that the United States has instructed Verizon not to disclose, its implementation would violate federal law.

OPINION

Based on the facts and assumptions set forth in this Letter, and subject to the qualifications discussed in this Letter, we are of the opinion that implementation of the Proposal would violate one or more federal laws to which Verizon is subject.

We note that, notwithstanding our analysis and conclusions, a reviewing court's determination of the questions implicated here would be based on its own analysis and interpretation of the factual evidence before it and applicable legal principles.

We do not opine as to the outcome of any pending litigation.

This opinion shall not be relied on by any party other than Verizon or its respective successors and/or assigns without our prior written consent. We understand that you intend to attach a copy of this opinion to your letter concerning the Proposal to the Securities and Exchange Commission under the procedures set forth in 17 C.F.R. 240.14a-8, and we consent to the use of this opinion for that purpose.

Very truly yours,

WILMER CUTLER PICKERING
HALE AND DORR LLP

By: John A. Rogovin /BMB
John A. Rogovin, a Partner

Jonas D. Kron, Attorney at Law

P.O. Box 42093
Portland, Oregon 97242
(971) 222-3366
jdkron@kronlaw.net

January 23, 2007

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

Re: Shareholder Proposal of Thomas Van Dyck Submitted to Verizon Communications Inc. for inclusion in the 2007 Proxy materials.

Dear Sir/Madam:

I have been asked by As You Sow Foundation, on behalf of Thomas Van Dyck (hereinafter referred to as the "Proponent"), who is a beneficial owner of shares of Verizon Communications Inc. (hereinafter referred to as "Verizon" or the "Company") common stock, and who has submitted a shareholder proposal (hereinafter referred to as the "Proposal") to Verizon, to respond to the letter dated December 27, 2006 sent to the Office of Chief Counsel by the Company, in which Verizon contends that the Proposal may be excluded from the Company's 2007 proxy statement by virtue of Rules 14a-8(i)(2), 14a-8(i)(3), 14a-8(i)(6), 14a-8(i)(7) and 14a-8(i)(10). Based upon my review, it is my opinion that the Proposal must be included in Verizon's 2007 proxy materials and I respectfully request 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 Verizon's Assistant General Counsel Mary Louise Weber.

SUMMARY RESPONSE

Based upon Verizon's no action request letter and supporting materials, and upon a review of Rule 14a-8, it is my opinion that the Proposal must be included in Verizon's 2007 proxy materials for the following reasons:

1. The Proposal is focused on a significant social policy issue that transcends the ordinary business of the Company. In particular, customer privacy concerns related to government and private entities have the attracted widespread attention of Congress, the American public, and business interests to name a few. In addition, the Proposal does not delve into the minute details of Company's compliance policies; does not dictate any particular action or conduct related to ongoing litigation; and does not seek an evaluation of a specific legislative proposal.

2. The Proposal, if implemented, would not cause the Company to violate the law. First, the WilmerHale opinion letter is based on the false presumption that our Proposal does not allow Verizon to exclude government classified information. This presumption makes the WilmerHale opinion letter inapplicable to the Staff's analysis. Furthermore, it is evident from the *Hepting* case and other examples, that the Company is capable of discussing these matters without violating confidentiality requirements. Consequently, the Company has not pointed to any decided legal authority that implementation would violate the law.
3. By failing to address the Proponent's core concerns, Verizon has not substantially implemented the Proposal. In particular, the Company's website published privacy policies do not provide the *discussion* of the policy issues raised by the Proposal and are not written to address shareholder (as opposed to customer) concerns.
4. Contrary to Verizon's representations, the Proposal is not so vague that it would be impossible to implement. While the Company tries to confuse matters by questioning the meaning of certain terms, it is evident that their plain meaning provides shareholders and management with a clear understanding about what the Proponent is asking for. In addition, Staff rulings on many other no-action requests indicates that proponents need not provide precise definitions, but only need to use language that is reasonably clear. Under that standard, we believe the Proposal has struck the right balance between specificity and generality.

THE PROPOSAL

VERIZON – PRIVACY RIGHTS PROTECTION REPORT

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

The reputation and good standing of Verizon may be placed in jeopardy by reports that its subsidiary MCI may have voluntarily provided customer phone records and communications data to the National Security Agency (NSA); and

We believe this alleged practice is seen by millions of Americans, including customers, shareholders and employees of Verizon, as a violation of our customers' privacy expectations and basic right to have phone and email records kept confidential; and

Verizon management has not confirmed or denied reports that its long-distance carrier MCI released consumer data to the NSA. Multiple class action and other consumer lawsuits have been filed against Verizon which could result in millions of dollars in liabilities and defense fees; and

Our customers have the choice to go to other telecommunications companies if they do not agree with the company's practices and may do so. These events and the potential for legal liability could affect the long-term value of our company; and

We are also concerned about ongoing violations of customer privacy including pretexting. This practice was used by Hewlett-Packard management to obtain data on phone calls made by board members. Verizon President Lawrence Babbio is an HP board member. Shareholders deserve an explanation of how pretexting could have occurred under Mr. Babbio's watch on the HP board. We believe Verizon executives are fully aware of the illegality of pretexting as demonstrated by the Verizon Wireless lawsuit filed against the individuals who obtained its customers' cell phone records as part of the HP investigation; and

These issues pose questions in regard to general respect for the rule of law upon which our democratic system depends. In light of the potentially negative uses of today's technology, we believe it is important that Verizon re-examine the steps it takes to protect the values embodied in an individual's right to privacy.

RESOLVED: The 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 overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other government agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers.

SUPPORTING STATEMENT

We believe it will benefit society, our customers, shareholders and Verizon's long-term value for the company to take a leadership role as protector of privacy rights and to issue this report. The proponents urge a YES vote.

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 – the Terrorist Surveillance Program – was confirmed by President Bush soon after it was described in the press.

In May, 2006, it was reported in the press that Verizon 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. This program has been referred to as the Call Records Program.

Public knowledge of these two Programs immediately resulted in a major national controversy directly involving Verizon 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 class action lawsuits seeking damages that could run into the billions of dollars. As a defendant in these suits, it is our opinion that they represent a significant financial risk to the Company.

In September, 2006 the issue of pretexting, the practice of getting an individuals personal information under false pretenses, became the subject of national attention as a scandal erupted at H-P. During that month a steady stream of revelations documented how private investigators hired by H-P management had used pretexting to investigate H-P board members. The furor eventually lead to Congressional hearings, state and federal investigations, and, just last week, President Bush signing the Telephone Records and Privacy Protection Act of 2006. The issue has also resulted in numerous lawsuits with Verizon as both a plaintiff and a defendant.

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

Furthermore, the goal of this Proposal is, as is the purpose of Rule 14a-8,[1] to facilitate a discussion between shareholders and management; and amongst shareholders about the significant policy issues facing the Company related to privacy concerns. When a company is faced with questions of such importance, shareholders have a right to communicate with management and other shareholders through the proxy materials. Mr. Van Dyck, as a shareholder, is exercising his rights through this Proposal.

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

ANALYSIS

I. Rule 14a-8(i)(7): 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. Under these circumstances the shareholders have an appropriate and legitimate role to play. Consequently, pursuant to the ordinary business exclusion, management's role must yield to the rights of shareholders to raise, consider and opine on those matters

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

which have significant social consequences.

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

A proposal cannot be excluded by Rule 14a-8(i)(7) if it focuses on significant policy issues. As explained in *Roosevelt v. E.I. DuPont de Nemours & Company*, 958 F. 2d 416 (DC Cir. 1992) a proposal may not be excluded if it has "significant policy, economic or other implications". *Id. at 426.* Interpreting that standard, the court spoke of actions which are "extraordinary, i.e., one involving 'fundamental business strategy' or 'long term goals.'" *Id. at 427.*

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

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

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

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

> Subject Matter of the Proposal: "Certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight. Examples include the management of the workforce, such as hiring, promotion, and termination of employees, decisions on the production quality and quantity, and the retention of suppliers. However, ***proposals relating to such matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable***, because the proposals would transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote." 1998 Interpretive Release (emphasis added)
>
> "Micro-Managing" the Company: The Commission indicated that shareholders, as a group, will not be in a position to make an informed judgment if the "proposal seeks to `micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Such micro-management may occur where the proposal "seeks intricate detail, or seeks specific time-frames or methods for implementing complex policies." However, "timing questions, for instance, could involve

> significant policy where large differences are at stake, and proposals may seek a reasonable level of detail without running afoul of these considerations."

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

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

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

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

Consequently, when analyzing this case, it is incumbent on Verizon to demonstrate that the Proposal does not involve any substantial policy or other considerations. Therefore, it is only if Verizon 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 Proponent and tends towards allowing, rather than excluding, the Proposal.

It would appear from Verizon's letter that it has implicitly conceded that the Proposal is focused on a significant social policy issue. Verizon's only discussion of the significant social policy question is when it cites to *Phillip Morris Companies, Inc.* (February 4, 1997) on page 5 for the proposition that even a proposal focused on a significant policy issue can still be excluded as relating to ordinary business. However, *Phillip Morris Companies, Inc.* does not apply to this case because it does not represent the current state of Rule 14a-8(i)(7) law. Specifically, that case precedes the 1998 Interpretive Release which made it clear that:

> proposals relating to such matters (day-to-day matters such as management of the workforce, such as hiring, promotion, and termination of employees, decisions on the production quality and quantity, and the retention of suppliers) 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.

As the SEC stated in this quote, if a proposal focuses on a significant social policy issue it thereby transcends the day-to-day business matters of the company and is appropriate for consideration by the shareholders. *Phillip Morris Companies, Inc.* represents an application of the Rule that was rejected in the 1998 Interpretive Release and therefore cannot be used as justification to exclude the Proposal.

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

- A May 2006 Gallup Poll found that 67% of Americans say that they are very closely or somewhat closely following reports that "a federal government agency obtained records from three of the largest U.S. telephone companies in order to create a database of billions of telephone numbers dialed by Americans" http://www.galluppoll.com/content/default.aspx?ci=5263. Exhibit 1. This is consistent with a December 2005 poll by the Rasmussen Report which concluded that "Sixty-eight percent (68%) of Americans say they are following the NSA story somewhat or very closely." http://www.rasmussenreports.com/2005/NSA.htm. Exhibit 2. This clearly demonstrates that the issue has persistent and widespread interest in American society.

- The issue has resulted in numerous reports by print, radio, television and Internet media. Attached in Exhibit 3 is a partial list of more than 40 stories on the issue from media outlets including the New York Times, USA Today, Wired Magazine, CBS, CNN and National Public Radio.

- The issue has been the subject of substantial interest by politicians and regulators. During the 109th Congress, the Senate Judiciary Committee subpoenaed the heads of several telecommunications companies to testify about the program and it was only at the behest of the Vice President of the United States that hearings on this issue were temporarily halted. John Diamond, *Specter: Cheney put pressure on panel*, USA Today, June 7, 2006; John Diamond, *Senators won't grill phone companies*, USA Today, June 7, 2006.

- Senator Patrick Leahy, (D-VT), the incoming chairman of the Senate Judiciary Committee, has expressed concern about the need for the companies allegedly involved to be held accountable if wrongdoing is found. "These companies may have violated the privacy rights of millions of Americans," Leahy said. "Immunity as a general rule in any industry can be a dangerous proposition for it promotes less accountability." Rebecca Carr, *Bush is seeking immunity for telecom industry*, Cox News, November 15, 2006.

- Several key national politicians and regulators have called for investigation into the scandal including Federal Communications Commissioner Michael Copps (Exhibit 4) and Representative Edward Markey (D- MA) (Exhibit 5), the then ranking minority member of the House Subcommittee on Telecommunications and the Internet.

- State utility regulators have also devoted substantial time and attention to the issue. Investigations of the telecommunications companies phone record sharing have been instituted in Vermont, Maine, New Jersey, Connecticut, and Missouri. Exhibit 6. Hearings on the issue have been held in a number of other states including Washington, Delaware, Nebraska, and Pennsylvania. Exhibit 7.

- The possibility that Verizon has shared phone records has also exposed the company to substantial potential liability. Class action lawsuits have been filed seeking damages for tens of millions of customers that could run to billions of dollars.

- 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., Verizon Communications Inc. and Bell-South Corp."

http://www.msnbc.msn.com/id/12771821 Exhibit 8.

- At Cisco Systems, Inc.'s November 2006 Annual Meeting, a shareholder proposal asking the company to address "steps the company could reasonably take to reduce the likelihood that its business practices might enable or encourage the violation of human rights, including freedom of expression and privacy . . ." received a noteworthy ***29% of the vote***. http://www.bostoncommonasset.com/news/cisco-agm-111506.html Exhibit 9. This vote is a clear expression of considerable shareholder concern about the role that technology and communications companies play in the freedom of expression and privacy.

Specifically on the issue of pretexting, the following are additional examples of the widespread concern about the issue, and Verizon's involvement:

- The issue came to national attention when a "public furor" erupted over the use of pretexting in an investigation at Hewlett-Packard. Pete Carey and Therese Poletti *HP's General Counsel Quits, Declines to Testify at Congressional Hearing* San Jose Mercury News September 28, 2006. Exhibit 10.
- Not only did the issue result in criminal investigations, but it also was the subject of closely watched congressional hearings. *Id* and Yuki Noguchi and Ellen Nakashima *House Panel Digs Deep in HP Spy Case* Washington Post, September 29, 2006. Exhibit 11.
- Verizon, specifically, became associated in the business press with the scandal. See Lorraine Woellert *Verizon Caught in HP Pretexting Web* Business Week Online, September 18, 2006. Exhibit 12.
- The issue has also been the subject of Federal Communications Commission ("FCC") interest pre-dating the HP scandal (Exhibit 13 Statement of FCC Commissioner Adelstein) and, according to Chairman Kevin Martin, the FCC has been "investigating the telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers,". Pamela Yip *Pretexting the latest identity* threat, Dallas Morning News, January 1, 2007. Exhibit 14.

B. The Proposal Addresses Customer Information Protections and Legal Compliance in a Permissible Fashion.

Verizon argues that the Proposal is excludable because it involves internal operating policies, customer relations and legal compliance programs – specifically the policies and procedures for protecting customer information. The Company's argument rests on the premise that "Management is in the best position to determine what policies and procedures are necessary to protect customer privacy and ensure compliance with applicable legal and regulatory requirements." Company Letter at page 4.

First, because of the Company's involvement in the Programs and rising concerns about pretexting, management is no longer in the best position to address customer privacy issues. As discussed earlier, Rule 14a-8(i)(7), 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. *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877 (S.D.N.Y. 1993) and *Medical Committee for Human Rights v. SEC*, 432 F. 2d. 659 (1970), vacated and dismissed as moot, 404 U.S. 402 (1972).

Second, there is nothing in the Proposal that seeks to delve into the *details* of internal operating policies, customer relations or legal compliance. As the SEC made clear in the 1998 Release, proposals may not "prob[e] 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." The Proposal expressly avoids this pitfall by focusing on the "overarching technological, legal and ethical policy issues." It is fair to assume that if we had sought a higher level of detail than this, that Verizon would have accused us of attempting to micro-managing the Company. To the contrary, the Proposal strikes the appropriate balance by focusing on the policy level issues while providing sufficient guidance so that the shareholders and management understand what is being requested.

Third, even assuming that the Proposal seeks direct involvement in compliance mechanisms there are many examples where the Staff has determined that it is appropriate for a shareholder proposal to address operating policies and legal compliance issues. In *Dow Chemical Company*(February 28, 2005) the Staff permitted a proposal that sought an analysis of the adequacy and effectiveness of the "company's internal controls related to potential adverse impacts associated with genetically engineered organisms". The allowed *Dow* proposal is analogous to our Proposal because both proposals seek a discussion about how the company is addressing a significant policy issue – adverse impacts associated with genetically engineered organisms on the one hand and customers' privacy rights on the other.

In *Bank of America Corp.* (February 23, 2006) the Staff denied a no-action request for a shareholder proposal which requested that this company's board "develop higher standards for the securitization of subprime loans to preclude the securitization of loans involving predatory practices" (an illegal practice). The company challenged the proposal on the grounds that the proposal dealt with "a general compliance program" because it sought to ensure that the company did not engage in an illegal practice. The Staff rejected that reasoning and we respectfully submit that the Staff should do so again. See also *Conseco, Inc.* (April 5, 2001) and *Assocs. First Capital Corp.* (March 13, 2000).

In *3M* (March 7, 2006) the Staff allowed a proposal that asked "the Board of Directors to make all possible lawful efforts to implement and/or increase activity on each of the principles named above in the People's Republic of China" including principles that addressed compliance with "China's national labor laws." See also *V.F. Corp* (February 14, 2004) and *E.I. du Pont de Nemours* (March 11, 2002). Similarly. in *Kohl's Corp.* (March 31, 2000) the Staff allowed a proposal that sought a report on the company's vendor standards and compliance mechanisms in the countries where it sources.

In *Dillard Department Stores, Inc.* (March 13, 1997) the company failed to persuade the Staff to exclude a proposal that asked for a report which described the company's actions to ensure that it would not do business with foreign suppliers who manufacture items using forced labor, convict labor or illegal child labor or fail to satisfy other applicable laws and standards.

In *Citigroup Inc.* (February 9, 2001) the Staff permitted a proposal that requested a report to shareholders describing the company's relationships with any entity that conducts business, invests in or facilitates

investment in Burma. It also sought specific information about the company's relationship with Ratchaburi Electricity Generating Co. of Thailand, as well as *explaining why these relationships did not violate U.S. government sanctions.*

What all of these proposals have in common with the Proposal is that they were addressing significant social policy issues confronting the company. Consequently, they were appropriate issues for shareholder consideration even if, arguably, they involved compliance issues. Whether they addressed genetic engineering, sweatshop/forced labor or predatory lending, the Staff concluded that those proposals were not concerned with mundane company matters, but were focused on how the company should address the issues which transcended the day-to-day affairs of the company.

With respect to the cases cited by the Company it is clear that the following do not apply because they all expressly involved making explicit changes to specific compliance mechanisms or policy at the company: *H&R Block Inc.* (August 1, 2006); *Bank of America Corporation* (March 3, 2005); *Deere & Company* (November 30, 2000); *Associated First Capital Corporation* (February 23, 1999);[2] *Chrysler Corp.* (February 18, 1998); *Citicorp* (January 9, 1998); and *Consolidated Edison Inc.* (March 10, 2003). In contrast, the Proposal is focused on a policy level discussion of technological, legal and ethical issues and does not direct the Company to adopt any specific compliance mechanism or policy.

As for *CVS Corp.* (February 1, 2000), that excluded proposal is distinguishable because it was a very broad proposal that was not limited to a specific significant policy issue, but rather related to "this company preparing for shareholders an annual strategic plan report describing its goals, strategies, policies and programs, and detailing the roles of its corporate constituents." The Proposal is not open ended like *CVS Corp.* and therefore is not analogous to that proposal.

Bank of America Corp. (February 21, 2006) and (March 7, 2005) are different than the Proposal because they simply requested a mere cataloging of existing policies and procedures for ensuring confidentiality. This Proposal, in contrast, goes beyond such a day-to-day issue, and requests a discussion of overarching policy issues which necessarily implies a discussion of potential additional policies. Our Proposal does not simply focus on a mundane matter like describing existing policies or mere procedural issues, but rather focuses on the significant policy issues of the societal and business concerns facing the Company as the result of the public and legal allegations relating to the Programs.[3] The same analysis applies as well to *Citicorp* (January 8, 1997).

Finally, 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. Like *Cisco*, the current Proposal focuses on how the company will address the central role it plays as a gatekeeper of individual's private information. Both proposals also addressed the issue in terms of privacy rights and we respectfully request the Staff to apply consistent reasoning by denying Verizon's no-action request.

---

2 Contrary to Verizon's description it is evident that the proposal was not limited to monitoring and reporting but related "to this company forming an independent committee of outside directors to develop and enforce a policy of preventing predatory lending practices which may violate federal or state law and report to shareholders."

3 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.

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

The Company also asserts that the Proposal is excludable as affecting its litigation strategy and the discovery process of numerous proceedings. First, it should be noted once again that the Proposal allows the Company to exclude "confidential information," which includes matters of litigation strategy and discovery related issues. Nowhere does the Proposal, expressly or implicitly, require a report on how the Company plans to argue the procedural or substantive aspects of any legal case or how it expects to resolve the cases. Instead what is contemplated by the Proponent is reporting on the overarching policy issues. 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 this Proposal.

Reynolds American Inc. (February 10, 2006). In that case, the proposal requested the company "undertake a campaign aimed at African Americans apprising them of the unique health hazards to them associated with smoking menthol cigarettes" while at the same time the company was a defendant in a lawsuit in which the Company was disputing " the use of menthol cigarettes by the African American community poses unique health risks to this community." In other words, if the proposal was enacted, the Company would have directly conceded the central point of the litigation and essentially mooted the litigation. Examining the Proposal in light of this case, an analogy would exist only if the Proposal sought the Company make some sort of statement that it has (as it characterizes the lawsuits) "violated consumer privacy rights". This is not what the Proposal does. Our Proposal requests an overarching policy discussion of the issues surrounding privacy rights and does not request the Company come to any particular conclusion regarding those rights and does not seek thereby to dictate the results of the lawsuits. Consequently, *Reynolds* cannot provide a basis for exclusion. See also *Loews Corporation* (March 22, 2006).

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

> 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's argument to be valid, the Proposal would need to somehow result in the litigation being resolved. Clearly a request for an overarching policy discussion of privacy issues as they relate to cooperating with local, state and federal authorities does not directly or indirectly dispose of any litigation the Company is engaged in.

R.J. Reynolds Tobacco Holdings, Inc. (March 6, 2003). Here, the resolution was designed to resolve the pending litigation against the company regarding its smuggling practices. In particular, the resolution required the company to "determine the extent of our Company's past or present involvement directly or indirectly in any smuggling of its cigarettes throughout the world." The litigation pending against the company was seeking precisely these outcomes. So implementation of the resolution could have effectively meant resolving the

litigation. In other words, this resolution fit into the ordinary business precedents "when the subject matter of the proposal is the same or similar to that which is at the heart of litigation in which a registrant is then involved." That is far from the situation in our resolution. The Proposal does not request, directly or even indirectly, any assessment about the litigation nor require any outcome to the litigation.

Similar conclusions must also be reached upon thorough review and analysis of the two other cases cited by the Company on pages 5 and 6 of its letter. As the Company made very clear in its brief descriptions of the cases, they were both 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***) and *Microsoft Corporation* (September 15, 2000) (asking the company ***to sue the federal government***). The Proposal, however, does not expressly, let alone impliedly, request the Company to bring an action in court, to sue anyone 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. Similarly, because our Proposal does not request any information about litigation (due to the confidentiality provision) and does not direct any litigation action, 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 a 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 the 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 the resolution has nothing to do with lobbying/litigation strategies.

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

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

Finally, the Company makes the specious 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 Verizon's business operations. It is evident from a number of previous Staff decisions that it is permissible to file a proposal that would involve a company in the political or legislative process. 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 held permissible.)

Turning to the cases cited by Verizon, it is evident that they do not apply because they sought an evaluation, expressly or implicitly, of specific legislative or regulatory proposals. *Microsoft Corporation* (September 29, 2006), as the Company pointed out, was excluded because it sought a report that evaluated the costs and benefits to the company of the "Net neutrality" legislative proposal. Similarly *Verizon Communications Inc.* (January 31, 2006) was excluded because it sought an evaluation of the impact of the flat tax proposal on the company. Our Proposal is distinct from these two proposals because it does not ask Verizon to evaluate the impact of any legislative proposal on the Company.

The proposal in *International Business Machines Corp.* (March 2, 2000), cited by the Company, requested:

> 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. Our 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".

This analysis is borne out in *Pepsico, Inc* (March 7, 1991), *Dole Food Company* (February 10, 1992) and *GTE Corporation* (February 10, 1992) all three of which requested the evaluation of the impact on the company of various federal health care proposals. Those proposals were all properly excluded because they sought an evaluation the specific impact of a legislative proposal on the company. The current Proposal, in contrast, does not do this even impliedly and therefore these three cases cannot provide the grounds for exclusion.

Finally, *Pacific Enterprises* (February 12, 1996) was properly excluded because it directed the regulatory, legislative and legal departments to undertake highly specific steps related to deregulation. Specifically, the proposal stated:

> Pacific Enterprises and Southern California Gas Company will dedicate the full resources of their regulatory, legislative and legal departments to the task of ending California utility deregulation. This effort will include lobbying in favor of laws (such as California Assembly Bill 1914 by Assembly Member Martha Escutia) mandating that any company transporting, distributing, storing or selling natural gas in the state of California must furnish the high standard of safety related services to the general public as has been provided by related public utilities before CPUC required implementation of utility deregulation.

Our Proposal is completely different from *Pacific Enterprises* because it does not direct any particular legislative result. Rather the Proposal seeks a discussion of the issues without a predetermined finding let alone a predetermined legislative result. Furthermore, the Proposal does not advocate for any specific legislation or set any criteria for legislation that Verizon should or must support. As a result, *Pacific Enterprises* does not apply to this case.

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

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

The Company argues that if it implemented the Proposal, that it would cause the Company to disclose government-classified information or material in violation of federal law. This argument fails for a number of reasons.

First, the WilmerHale letter incorrectly assumes that the term "confidential" does not mean government-classified information and therefore is asking for the Company to disclose information that could jeopardize the nation's security and violate federal law. Because the WilmerHale letter is entirely based on this assumption, its analysis is extraneous to the issues before the Staff. As WilmerHale puts it "nor does this Letter address this possible interpretation" (i.e. the exclusion of government-classified information). Since the letter does not address the correct meaning of the Proposal it is not applicable to this case and the Company's entire Rule 14a-8(i)(2) argument is unsupported.[4] Therefore, because our Proposal specifically allows Verizon to exclude confidential information, it will not cause the Company to disclose classified information or materials and will not cause a violation of the law.

It is not at all clear why WilmerHale interprets the term "confidential" to only refer to intellectual property and trade secrets. The plain meaning of "confidential" includes government classified information and there is no reason to assume that the Proponent did not intend that meaning. For example, The American Heritage Dictionary of the English Language Fourth Edition, 2000 at page 386 defines "confidential" as inter alia "Containing information, the unauthorized disclosure of which poses a threat to national security." See also Merriam-Webster.com which defines "confidential" as "containing information whose unauthorized disclosure could be prejudicial to the national interest". Given this analysis the Company's fall back position appears to be (on page 11) that "the result would be an entirely abstract study" that is vague and indefinite. As argued fully below, that contention fails because the Proposal has struck the appropriate balance by avoiding being too general and too specific.

We would like to take this opportunity, however, to point out that the subject matter of the Proposal is clearly within the range of information that can be discussed legally. While the WilmerHale letter claims that there is a broad ban on any discussion of the Programs, it is clear that this is not the case. The Hon. Judge Vaugh T. Walker, the judge assigned by the Judicial Panel on Multidistrict Litigation to hear the consolidated lawsuits related to claims against the telecommunications companies including Verizon, has concluded

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

The Hon. Judge Vaugh R. Walker's July 20, 2006 Order in Hepting v. AT&T Corporation at p. 29 (emphasis added) Exhibit 15. While this order in *Hepting* applies only directly to AT&T, the Hon. Judge Walker will be making a determination regarding Verizon in February or March and the order gives a very clear indication about how he views these issues.

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

4 We note that on page 8, the Company concedes that the request regarding pretexting "would not result in a violation of law".

The Hon. Judge Walker also made the following point:

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

Id at pages 39 – 40.

Consequently, the issue whether or not the Company provided customer telephone records to the Government can hardly be called a state secret and is something that can be discussed in general terms.

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

> Nothing in this Letter should be construed as an admission or denial of Verizon's involvement in the Alleged Programs. For the purposes only of responding to your request, we accept at face value the facts asserted in the media reports. No inference regarding the truth of the reports can be drawn from these assumptions, nor should anything in this Letter be construed as an admission or denial of Verizon's involvement in the Alleged Programs.

It is assumed that any report to shareholders would contain the same or similar language making clear that the Company cannot (absent permission from the government) discuss the *details* of an intelligence program or disclose its existence. However, the parameters of such a discussion – the importance of privacy versus national security and the responsible role of a corporation in weighing those two values – is clear. There is nothing confidential about the law surrounding the sharing of telephone information.

We note, however, that it is odd that the Company has stated that it cannot admit or deny Verizon's involvement in the Alleged Programs because Verizon has made a public declaration denying any involvement in the Programs. See FoxNews: *Verizon- We Didn't Give Customers' Call Records to NSA Either*, May 16, 2006 <http://www.foxnews.com/printer_friendly_story/0,3566,195745,00.html>. Exhibit 16.

As the Hon. Judge Walker observed:

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

Walker Order at page 41.

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 any law being applied to shareholder proposals or other provisions of the proxy rules. Furthermore, they have not established any decided legal authority on this issue. In fact, the Hon. Judge Walker's Order indicates that the Company's assertions of the law are misplaced and that the decided legal authority runs contrary to their position. Consequently, the Company has not met its burden and we respectfully request the Staff conclude that Rule 14a-8(i)(2) does not apply to this Proposal. In the alternative, and in light of *The Quaker Oats Company,* we request that the Staff not express any view with the respect to the application of Rule 14a-8(i)(2).

III. Verizon's privacy policies for customers are not substantial implementation of the Proposal because the Proposal seeks a *discussion* of privacy issues with *shareholders*.

The Company claims that the Proposal's request has been substantially implemented through the privacy policies it publishes on its websites. However, based on a review of the websites and the applicable no-action letters issued by the Staff it is clear that the Verizon 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 those websites clearly do not address the concerns raised by the Proponent. For example, the www.verizon.com privacy policy link makes only cursory and conclusory mention of when Verizon would disclose customer information and makes no mention about disclosing communications content. On that website the only statements that could be said to be covered by the Proposal are the following:

> However, we do release customer information without involving you if disclosure is required by law or to protect the safety of customers, employees or property.
>
> **
>
> When you dial 911, information about your location may be transmitted automatically to a public safety agency.
>
> **
>
> Verizon must disclose information, as necessary, to comply with court orders or subpoenas. Verizon also will share information to protect its rights or property and to protect users of its

services and other carriers from fraudulent, abusive or unlawful use of services.

**

We may, where permitted by law, provide information to credit bureaus, or provide information and/or sell receivables to collection agencies, to obtain payment for Verizon billed products and services.

This is far removed from a discussion of "the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other government agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers." In fact there is no discussion of the technological or ethical policy issues surrounding disclosure. While the words "law", "court orders" and "subpoenas" appear in the policy, this is clearly not a discussion of the policy issues at stake. Given that this website is representative of the other websites identified by the Company it would appear that all of Verizon's statements fail to address the Proposal's requests. See Exhibit 17 for additional excerpts from the websites.

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. This Proposal does not ask for a specific result or policy, but an exploration of the issues as they apply to Verizon's policies and future as a profitable and responsible company. Clearly Verizon's privacy policies do not do that.

Furthermore, these websites are 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 our customers. For example, it would be nonsensical to discuss the merits of a variety of privacy protection technologies or policies 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. This would provide shareholders with documentation of management's discussion in a unified manner, rather than over multiple websites often 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 Verizon 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 Verizon'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.

IV. Vagueness: The Proposal has struck the proper balance between specificity and generality, therefore the Company has the power, authority and ability to implement it.

Verizon argues that the Proposal is so vague that it is impossible to implement. In particular the Company argues

- that the Proposal fails to define the terms "confidential" and "technological" and
- exclusion of classified information and the request for a discussion of "overarching" policy issues would result in an entirely abstract study that is not suited for a corporate report to shareholders.[5]

Under Rules 14a-8(i)(3) and 14a-9, proposals are not permitted to be "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 exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (September 15, 2004) ("SLB 14B") However, the SEC has also made it clear that it will apply a "case-by-case analytical approach" to each proposal. Exchange Act Release No. 34-40018 (May 21, 1998) ("1998 Interpretive Release"). Consequently, the vagueness determination becomes a very fact-intensive determination in which the Staff has expressed concern about becoming overly involved. SLB 14B. Finally, the Staff stated at the end of its SLB 14B vagueness discussion that "rule 14a-8(g) makes clear that *the company bears the burden* of demonstrating that a proposal or statement may be excluded." *Id* (emphasis added).

Addressing Verizon's first argument, previous Staff letters indicate that there is no requirement that proposals define specific terms in a proposal so long as the concept was readily understandable. For example, in *Kroger Co.* (April 12, 2000) the 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 the company did not have the

5 We observe that the first and fourth bullets on pages 11 and 12 do not provide any reasoning as to why they would be the basis for exclusion. Rather they attempt to characterize, inaccurately, the intention of the Proposal in an apparent attempt to cast aspersions on the Proponent's intentions.

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's use of the word "confidential" 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 at 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.

Also, 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 Proponent in this case now before the Staff has addressed the issue in a reasonable fashion. There is no need to create ambiguities where none exist.

Finally, consider *Microsoft Corporation* (September 14, 2000) in which the Staff required inclusion of a proposal that requested the board of directors to implement and/or increase activity on eleven principles relating to human and labor rights in China. In that case, the company argued "phrases like 'freedom of association' and 'freedom of expression' have been hotly debated in the United States" and therefore the proposal was too vague. Similarly, Verizon's claim that our Proposal is meaningless because it seeks to address large issues like the right to privacy should not succeed.

As discussed earlier, the plain meaning of the term "confidential" includes classified information and there is no reason to conclude this will confuse or mislead shareholders. 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. In addition, the Proposal makes clear that it is not seeking a high level of specificity or intricate detail. In fact, Verizon's shareholders will understand that the Proposal requests a general discussion of the issues and does not seek to elicit confidential information. As stated in the Proposal, shareholders request a report "excluding confidential and propriety information".

With respect to the term "technological" we believe Verizon is trying to create confusion where none exists. The word is defined by The American Heritage Dictionary of the English Language Fourth Edition, 2000 at page 1777 as "relating to or involving technology". See also www.merriam-webster.com "of, relating to, or characterized by technology". Applying this definition it is understandable that the Proposal is requesting a discussion of the technology issues related to the disclosure of customer records and communications content. We think it is abundantly clear that telephone and internet communications are completely reliant on technology and therefore the report would necessarily include a discussion of

technology. How this concept will confuse shareholders and therefore make the Proposal impossible to implement it not at all apparent. Again, Verizon is trying to create confusion where there is none.

Turning next to the claim that the Proposal will result in an abstract report that is not appropriate for a corporate report to shareholders we demonstrate below that the report would not be a meaningless intellectual exercise. Rather, it would provide shareholders with useful information, would document management's consideration of these significant social policy issues and provide the basis for a meaningful dialogue between Verizon and its shareholders.

If the Company were to implement the Proposal, there are many subjects it could discuss without disclosing classified information and still provide relevant information to shareholders. For example, Verizon, under the subject of the legal issues surrounding the disclosure of customer records and communications content, could discuss the necessary trade offs the Company will have to consider in light of the societal benefits of strong privacy protections and the needs for homeland security. In that discussion it could discuss the various ways different companies such as Qwest, AT&T, Cisco, Microsoft, Yahoo, or AOL have handled such trade offs. By considering the business practices of other companies, Verizon shareholders and management will be better able to decide how Verizon should address this significant policy issue and from a policy perspective discuss how to chart the Company's future. None of that discussion would require any disclosure of classified information whatsoever and yet would be very useful information for shareholders as they evaluate the Company's future, its commitment to responsible behavior and their investment in Verizon.

Another possibility would be a discussion of the feasibility of the Company contributing to technological advancements which would allow the company to assist law enforcement more effectively and do so with even stronger protections of civil liberties. Similarly, Verizon could report on technological advancements that would cut down on pretexting. Such developments would give the company a business advantage as customers would be attracted to such protections and it would serve to improve the Company's standing as a defender of American security and liberty. It could also bring with it other technological advances that may offer other business opportunities. This is information that would be useful for shareholders as they discuss these issues with the Company and evaluate how the Company, at a broad policy level, proceeds.

Also, there is nothing confidential about the laws themselves that apply to Verizon. The Company could readily discuss the contours and various interpretations of the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act of 1978, the Telephone Records and Privacy Protection Act of 2006, the Telecommunications Act of 1996 and the Electronic Communication Transactional Records Act. This discussion would not need to be an abstract law review, but could easily involve a discussion of the business implications and alternatives for the Company under these laws. Such an analysis could also serve as documentation that management has evaluated the feasibility of different ways to negotiate its relationship with the government. In light of the public furor and ensuing litigation, shareholders are right to ask whether the Company has struck the right balance and what will be necessary to do so in the future.

It is clear that excluding confidential information will not result in a meaningless and abstract "white paper." The challenges posed by privacy issues are significant, and ask shareholders, in the words of one court, to fulfill their "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). Furthermore, they offer the Company an opportunity to become

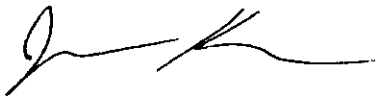
a better, more efficient and more competitive company.

Therefore, it is apparent that Verizon has not met its significant burden of proving that under Rules 14a-8(i)(3) and 14a-9 the Proposal should be excluded. The above discussion demonstrates that the plain meaning of the words in the Proposal will not create confusion for shareholders, directors or management and that the requested report would provide a meaningful and useful report that would be appropriate for shareholders. Consequently the Proposal would not be impossible to implement.

CONCLUSION

In conclusion, I respectfully request the Staff to inform the Company that Rule 14a-8 requires denial of its no-action request. As demonstrated above, the Proposal is not excludable under any of the criteria of Rules 14a-8 or 14a-9. In the event that the Staff should decide to concur with the Company and issue a no-action letter, I respectfully request the opportunity to speak with the Staff. Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Jonas Kron
Attorney at Law

Enclosures

cc: Mary Louise Weber, Assistant General Counsel, Verizon Communications Inc.
As You Sow Foundation
Thomas Van Dyck

Exhibits

1. May 2006 Gallup Poll.
2. December 2005 Rasmussen Report Poll.
3. List of media reports.
4. Statement of Federal Communications Commissioner Michael Copps.
5. May 15, 2006 letter from Representative Edward Markey (D- MA).
6. *Petition of Vermont Department of Public Service* Docket No. 7193.
7. *ACLU of Pennsylvania v. AT&T Communications of PA, LLC, et al.*
8. May 2006 Newsweek Poll.
9. Boston Common Asset Press Release.
10. *HP's General Counsel Quits, Declines to Testify at Congressional Hearing* San Jose Mercury News September 28, 2006.
11. Yuki Noguchi and Ellen Nakashima *House Panel Digs Deep in HP Spy Case* Washington Post, September 29, 2006.
12. Lorraine Woellert *Verizon Caught in HP Pretexting Web* Business Week Online, September 18, 2006.
13. Statement of FCC Commissioner Adelstein.
14. Pamela Yip *Pretexting the latest identity* threat, Dallas Morning News, January 1, 2007.
15. *Hon. Judge Vaugh R. Walker's July 20, 2006 Order in Hepting v. AT&T Corporation.*
16. FoxNews: *Verizon- We Didn't Give Customers' Call Records to NSA Either*, May 16, 2006.
17. Excerpts from Verizon's Privacy Policies.

EXHIBIT 1

THE GALLUP POLL®

SOURCE: Gallup Poll News Service

CONTACT INFORMATION: Media Relations 1-202-715-3030
Subscriber Relations 1-888-274-5447
Gallup World Headquarters
901 F Street, NW
Washington, D.C. 20004

Civil Liberties

Gallup's Pulse of Democracy

The Patriot Act and Civil Liberties

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

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

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

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

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

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

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

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

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

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

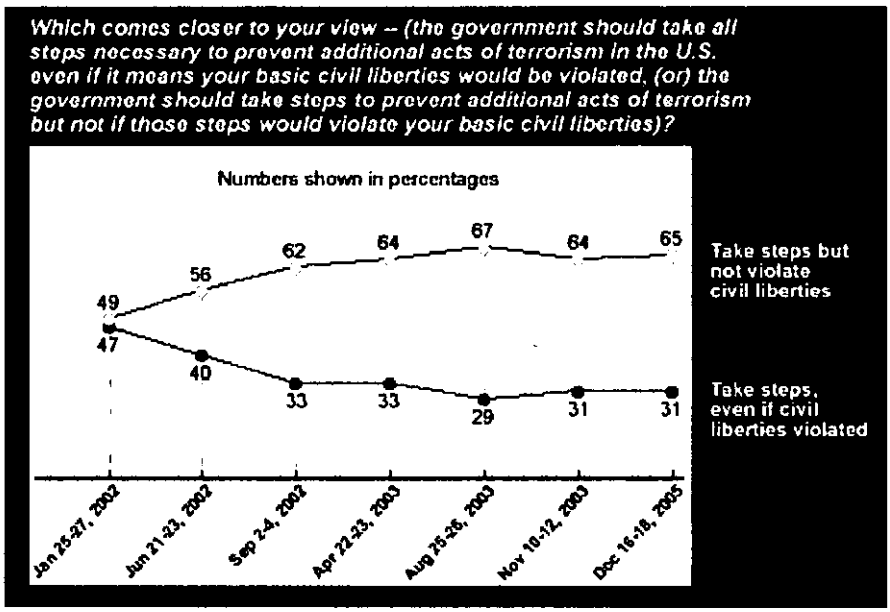
Key Subgroup Differences Views about the Patriot Act and civil liberties are highly partisan.

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

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

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

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



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

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

^ Asked of a half sample.

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

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

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

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

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

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

^ Asked of a half sample.

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

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

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

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

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

[ASKEDF OF ADULTS WHO APPROVE OF GOVERNMENT PROGRAM]

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

Do you think there would ever be circumstances in which it would be right for the government to create a database of telephone records, or would it not be right for the government to do this under any circumstances?

[ASKED OF ADULTS WHO DISAPPROVE OF GOVERNMENT PROGRAM]

	Yes, are	No, are not	No opinion
2006 May 12-13	34%	60	6

Based on what you have heard or read about this program, do you think it – [ROTATED: definitely violates the law, probably violates the law, probably does not violate the law, (or) definitely does not violate the law]?

	Definitely violates the law	Probably violates the law	Probably does not violate the law	Definitely does not violate the law	No opinion
2006 May 12-13	22%	32	25	14	8

If you knew that the federal government had your telephone records, how concerned would you be -- very concerned, somewhat concerned, not too concerned, or not concerned at all?

	Very concerned	Some-what concerned	Not too concerned	Not concerned at all	No opinion
2006 May 12-13	22%	13	20	44	1

If you knew that your telephone company had provided your telephone records to the federal government as part of this program, would you feel that your personal privacy had been violated, or not?

	Yes, would feel violated	No, would not	No opinion
2006 May 12-13	57%	42	1

Would you favor or oppose holding immediate Congressional hearings to investigate this program?

	Favor	Oppose	No opinion
2006 May 12-13	62%	34	4

How concerned are you that -- [ITEMS A-B ROTATED, ITEM C READ LAST]-- very concerned, somewhat concerned, not too concerned, or not concerned at all?

A. Based on this program, the government would misidentify innocent Americans as possible terrorist suspects

	Very concerned	Some-what concerned	Not too concerned	Not concerned at all	No opinion
2006 May 12-13	36%	29	21	14	1

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

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

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

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

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

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

^ Asked of a half sample.

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

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

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

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

^ Asked of a half sample.

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

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

^ Asked of a half sample.

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

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

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

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

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

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

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

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

2004 Feb 16-17	51%	34	15

C. Enter houses of worship or attend political rallies

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

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

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

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

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

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

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

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

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

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

^ Back to Top

EXHIBIT 2

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

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

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

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

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

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

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

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

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

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

EXHIBIT 3

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

Print and Electronic

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Lisle Brunner, *DOJ asks appeals court to block domestic surveillance lawsuit*, Jurist, December 5, 2006

Radio

1. Larry Abramson, *Phone Companies Deny Cooperating with NSA*, Weekend Edition, **National Public Radio**, May 20, 2006

2. Story, Morning Edition, **National Public Radio**, May 24, 2006

3. O. Kay Henderson, *ICLU Jumps Into Phone Records Debate*, **Radio Iowa**, May 24, 2006

4. Larry Abramson, Morning Edition, **National Public Radio**, May 25, 2006

5. Armstrong Williams and Sam Greenfield, WWRL Morning Show, **WWRL 1600**, May 25, 2006

Television

1. **MSNBC**, Dan Abrams Report, May 24, 2006

2. **CBS News**, The Early Show, May 24, 2006

3. **CNN**, News Report, May 25, 2006

4. **CNBC**, Morning Call, May 25, 2006

EXHIBIT 4

NEWS

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

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

FOR IMMEDIATE RELEASE
May 15, 2006

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

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

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

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

--FCC--

EXHIBIT 5

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE
RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–2107

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

DISTRICT OFFICES:
5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

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

May 15, 2006

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

Dear Mr. Chairman:

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

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

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

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

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

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

Thank you in advance for your attention to this matter.

Sincerely,

Ed Markey

Edward J. Markey
Ranking Democrat
House Subcommittee on
Telecommunications and the Internet

EXHIBIT 6

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

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)

EXHIBIT 7

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

EXHIBIT 8

MSN Tracking Image
MSNBC.com
Newsweek.com
Newsweek Poll: Americans Wary of NSA Surveillance
Bush's approval ratings hit new lows as controversy rages.
NEWSWEEK WEB EXCLUSIVE
By David Jefferson
Updated: 10:11 a.m. PT May 14, 2006

May 13, 2006 - Has the Bush administration gone too far in expanding the powers of the President to fight terrorism? Yes, say a majority of Americans, following this week's revelation that the National Security Agency has been secretly collecting the phone records of U.S. citizens since the September 11 terrorist attacks. According to the latest NEWSWEEK poll, 53 percent of Americans think the NSA's surveillance program "goes too far in invading people's privacy," while 41 percent see it as a necessary tool to combat terrorism.

President Bush tried to reassure the public this week that its privacy is "fiercely protected," and that "we're not mining or trolling through the personal lives of innocent Americans." Nonetheless, Americans think the White House has overstepped its bounds: 57 percent said that in light of the NSA data-mining news and other executive actions, the Bush-Cheney Administration has "gone too far in expanding presidential power." That compares to 38 percent who think the Administration's actions are appropriate.

There's more bad news for the White House in the NEWSWEEK poll: President Bush's approval rating has dropped to the lowest in his presidency. At 35 percent, his rating is one point below the 36 percent he received in NEWSWEEK's polls in March and November, 2005.

Iraq continues to be the biggest drain on the president's popularity: 86 percent of Americans say the Iraq situation, coupled with new information about the decision to go to war, have negatively influenced their view of the president. Asked about Bush's performance on a variety of issues, from the economy to taxes, respondents gave the president some of the worst marks of his tenure, and in no instance did approval reach more than 50 percent.

Anger over the recent spike in prices at the pump has cost the president dearly: only 17 percent of Americans approve of the way Bush is handling gas prices. Nor do they like the way he is dealing with the federal budget deficit (only 19 percent approve) or immigration policy (25 percent). Even as Congress was approving the latest Bush tax cuts this week, public opinion of his handling of taxes dropped to a record low for him of 39 percent. Half of Americans (50 percent) now think George W. Bush will go down in history as a "below-average" president.

News of the NSA's secret phone-records program comes at an especially awkward time for the president. His nominee for the top job at the CIA—former NSA head Gen. Michael Hayden—heads into confirmation hearings on the Hill next week. With Democrats expressing outrage over the surveillance program, and several Republicans voicing concern as well, the hearings could turn into something of a Congressional probe into the NSA's collection of phone data.

According to the NEWSWEEK poll, 73 percent of Democrats and 26 percent of Republicans think the NSA's program is overly intrusive. Details of the surveillance efforts were first reported on Wednesday by USA Today. The newspaper said the NSA has collected tens of millions of customer phone records from AT&T Inc., Verizon Communications Inc. and Bell-South Corp., in an effort to assemble a database of every call made within the United States. While the records include detailed information about when and where phone calls were made, the government isn't listening in to the actual conversations, a U.S.

intelligence official familiar with the program told the newspaper. The only big telecommunications company that has refused to participate is Denver-based Qwest, which says it was concerned about the legal implications of turning over customer information to the government without warrants.

The fracas over surveillance is yet another headache the Republicans didn't need heading into the November midterm elections. Seventy-one percent of Americans are dissatisfied with the way things are going in the country, and more than half—52 percent—say they would like the Democrats to win enough seats to take over Congress this November (only 35 percent want the Republicans to keep control). Looking ahead to the presidential race in 2008, more Americans said they would like to see a Democrat elected than a Republican—50 percent versus 31 percent. That, despite the fact that a majority of those polled don't believe a Democrat would do any better than Bush is doing on a variety of issues. Democrats also have a significant lead in being perceived as better able to bring about the changes the country needs: 53 percent to 30 percent.

Bush's new approval low of 35 percent in the NEWSWEEK poll is below the nadir of Bill Clinton's presidency in May 1993, when the former president hit 36 percent. The 41st president, George H.W. Bush, hit his lowest ratings late in 1992 before he was defeated by Clinton: A Gallup poll in July 1992 recorded a 32 percent approval rate for the first President Bush. But other presidents have fared worse. Jimmy Carter scored 28-29 percent in June and July 1979, according to Gallup. President Richard Nixon's Gallup number dropped to 24 percent in August 1974.

For the NEWSWEEK poll, Princeton Survey Research Associates International interviewed 1,007 adults aged 18 and older between May 11 and 12 by telephone. The margin of error is plus or minus 4 percentage points.

URL: http://www.msnbc.msn.com/id/12771821/site/newsweek/page/2/

EXHIBIT 9

BOSTON COMMON
ASSET MANAGEMENT, LLC

Home > News

Human Rights and Internet Fragmentation Proposal Receives Record Shareholder Support

BOSTON, MA November 15, 2006 -- The human rights and Internet fragmentation resolution led by Boston Common Asset Management received a record level of support from shareholders, according to the preliminary vote announced at the Cisco Systems Annual Stockholders Meeting today in Santa Clara, California. Twenty-nine percent of all shareholders voted against management's recommendation and supported Boston Common's proposal with a "For" or "Abstain" vote, according to an announcement made at the meeting. "This is a record vote for a resolution of this nature" said Dawn Wolfe, Social Research Analyst at Boston Common Asset Management. "The fact that well over one-quarter of all Cisco shareholders disagree with the company's assertion that Internet fragmentation and human rights liabilities do not represent a potential threat to Cisco's long term global growth is a strong statement," Wolfe continued.

The proposal, co-filed by four additional investors, asks management to disclose the concrete steps it could reasonably take to reduce fragmentation of the Internet, the suppression of information, or violations of personal privacy. Internet fragmentation, or balkanization, occurs when government authorities create extensive firewalls around citizens, severely restrict the flow of information, conduct pervasive surveillance of electronic communication users, and ultimately slow the growth of people accessing the Internet. Boston Common began formal engagement with Cisco in January 2005 over the human rights and long term financial impacts of selling powerful networking technology to repressive governments.

For more information please contact Dawn Wolfe, Boston Common Asset Management, (617) 720-5557, dwolfe(at)bostoncommonasset.com

84 State Street, Suite 1000, Boston, MA 02109
Tel: 617-720-5557 Fax: 617-720-5665

EXHIBIT 10

HP's General Counsel Quits, Declines to Testify at Congressional Hearing
By Pete Carey and Therese Poletti
San Jose Mercury News
September 28, 2006

Hewlett-Packard General Counsel Ann O. Baskins resigned today and told a Congressional subcommittee investigating HP's boardroom leak scandal that she would invoke her Fifth Amendment privilege and decline to testify at today's hearing.

Baskins said in a letter hand delivered to the House Energy and Commerce Committee that she believed that the company's use of deception to obtain private phone records during its investigation was legal. The deception -- called ``pretexting" -- had investigators impersonating HP board members, employees, reporters and others to obtain their private phone records without their knowledge.

She also submitted several documents, including a memo of an interview conducted by Wilson Sonsini of former HP lawyer Kevin Hunsaker. In that memo, the lawyers reported that Hunsaker told them HP had used pretexting in other, unrelated investigations, including one involving a subject who was going through a ``messy" divorce.

The subcommittee hearing today revealed at least one HP investigator tried to sound an alarm about the company's use of pretexting to obtain phone records, but apparently got nowhere.

A document released by the subcommittee showed that a member of the investigative team, Vince Nye, sounded a warning in a Feb. 7, 2006 e-mail to HP security manager Anthony Gentilucci.

`I have serious reservations about what we are doing," Nye wrote in an e-mail to Gentilucci. ``As I understand Ron's methodology in obtaining this phone record information it leaves me with the opinion that it is very unethical at the least and probably illegal. If it is not totally illegal, then it is leaving HP in a position that could damage our reputation or worse.

The e-mail continued, ``I am requesting that we cease this phone-number gathering method immediately and discount any of its information. I think we need to refocus our strategy and proceed on the high-ground course."

The ``Ron" referred to in Nye's e-mail was Ronald DeLia, head of a Boston-area private investigation firm who worked for HP's investigation and declined to testify today. Gentilucci resigned earlier this week as head of HP's global security unit in Boston, and he also declined to testify.

As the hearing opened, committee members expressed their disbelief that nobody at HP stepped forward to say the practice, legal or not, was unethical and should be stopped. Rep. John Dingell, D-Mich, called the HP actions ``a plumbers' operation that would make Richard Nixon blush, were he still alive," referring to the 1970s Watergate break-in scandal that brought down the Nixon presidency.

``The cure, in this case, appears to have been far worse than the disease, and now poses a far greater threat to Hewlett-Packard," Dingell said.

Since HP disclosed earlier this month it had hired outside investigators that used pretexting to trace boardroom leaks to reporters, the company has faced a public furor resulting in the resignation of its board chairman on Friday. The disclosure has triggered two criminal investigations and the congressional hearing today.

Several committee members used the opportunity to make another pitch for anti-pretexting legislation it sent to Congress in May, but which, as committee member Diana Degette, D-Colo., said seemed to have ``fallen down a black hole." Jan Schakowsky, D-Ill, said HP was invited to testify in July on how to raise the bar on protecting privacy. ``Little did we know that Hewlett-Packard had been engaging in the worst practices out there," she said.

Although Baskins did not testify, she gave the committee several documents backing up her claim to have repeatedly confirmed, through an HP lawyer, the legality of the methods used by HP investigators to obtain phone records of board members, HP employees and reporters.

In one document, former senior HP lawyer Hunsaker explained the process used by an outside private investigator, Ronald DeLia, of Boston-based Security Outsourcing Solutions.

``We provide DeLia the names and telephone numbers we are interested in, he passes the information to the third-party company, and they then make the pretext calls to the phone service providers," Hunsaker wrote to Baskins on May 1.

Hunsaker added, ``It should be noted that this is a common investigative tool that has been used by professional investigators and law firms for more than 20 years -- this fact was confirmed by discussing the issue with a number of experts in the field."

Hunsaker, referring to himself in the third person in the memo, said he had taken a number of steps to confirm the legality of the practice of pretexting, which involves an investigator posing as the target of an investigation to obtain access to the target's private phone records.

He said he was ``confident" that all phone records information obtained by HP's investigators were obtained ``in a lawful manner."

Memos describing interviews with Hunsaker by Wilson Sonsini lawyers revealed the law firm's own investigation of the HP leak probe in August. It said that Hunsaker told them he had done ``hundreds of investigations" but that this was the first one to involve the use of pretexting. He said he first learned about pretexting one or two years ago in connection with another HP investigation.

Hunsaker told Wilson Sonsini attorneys in an interview in August that he first learned HP had used pretexting to obtain phone records in July 2005 in connection with an unrelated HP investigation. A subject of that investigation ``was going through a messy divorce, and his attorney contacted HP and claimed that HP had changed his client's pin number in order to access his voice mail. Hunsaker's team told them they had not altered the subject's pin or voice mail, but had used pretexting to obtain phone information about the subject."

The memo also described how Hunsaker obtained reporters' phone numbers from HP's media relations department and gave them to DeLia.

Asked about his research into the legality of pretexting, Hunsaker said ``that he did about an hour's worth of online research."

The same document describes how Hunsaker had the hard drives of every member of HP's executive council ``imaged" as part of the investigation.

A month into the investigation, Dunn and Baskins asked Hunsaker to reconfirm the legality of the phone pretexting. The answer appears to have always been the same: it was legal.

California Attorney General Bill Lockyer has launched a criminal investigation of HP's investigative pretexting, saying several California laws make the practice illegal.

The Subcommittee on Oversight and Investigations of the House Committee on Energy and Commerce has been investigating the broader use of pretexting in hearings this year. Because the practice of pretexting is a focus of the hearings, several HP executives and private eyes involved in its leak investigation were invited to testify today.

Several wireless industry executives and government regulators have been invited to speak before the committee about pretexting Friday.

EXHIBIT 11

House Panel Digs Deep in HP Spy Case
Dunn, Hurd Shoulder Brunt of Tough Questioning at Hearing
By Yuki Noguchi and Ellen Nakashima
Washington Post Staff Writers
Friday, September 29, 2006; D01

Lawmakers fiercely challenged former Hewlett-Packard Co. chairman Patricia C. Dunn yesterday on her assertion that she did not know about potentially illegal tactics used in the company's spy scandal, while 10 other key figures in the case shunned interrogation by refusing to testify during a congressional hearing.

A total of 14 witnesses, flanked by their lawyers, came before a phalanx of House subcommittee members. Most of the seven hours of questioning was directed at Dunn, who coolly endured accusations that she aided or condoned a widespread surveillance campaign against HP board of directors, journalists and their families.

Despite being confronted with a copy of a memo saying it was "probable" that Dunn had been informed that pretexting -- impersonating people to obtain information -- was necessary to acquire phone records, Dunn repeatedly said she was not aware of the methods investigators used to obtain personal calling records while investigating leaks to the media.

Chief executive Mark V. Hurd, furrowing his brow and peering over his reading glasses, assumed more responsibility while denying knowledge of possible illegal tactics. He admitted that his lack of involvement contributed to an investigation that overreached and damaged the company's reputation.

"This is not my finest hour," he said, adding later, "I should have caught it, I didn't."

The day began with the resignation of HP general counsel Ann O. Baskins, a 24-year veteran of HP who, hours before testimony started, became the sixth major HP executive or board member to resign since HP disclosed early this month that its investigators might have illegally obtained private phone records.

Lawmakers confronted Baskins with handwritten notes, apparently written by her during a phone call or meeting, suggesting that she had encouraged investigators to "[c]all carriers Nextel, Sprint and use pretexts to extract info."

"Now this document and others show that you were aware that HP was engaging in pretexting," said Edward Whitfield (R-Ky.), chairman of the House Energy and Commerce oversight investigations subcommittee.

Baskins declined to answer, citing her Fifth Amendment right against self-incrimination.

One by one, nine other HP employees and outside contractors also pleaded the Fifth Amendment, remaining silent after being confronted with the most vivid evidence suggesting they knew or should have known about the questionable surveillance activities. Those declining to testify included the main architects of the leak probe, HP's chief ethics director Kevin Hunsaker and global security head Anthony Gentilucci, and six private detectives.

The California attorney general and the FBI are conducting criminal investigations.

Later Dunn, Hurd, HP information technology security head Fred Adler and outside counsel Larry Sonsini sat somberly as subcommittee members chastised and interrupted them for presiding over a probe that led the venerable Silicon Valley company into such unethical behavior as sending bogus information to a reporter, sitting outside of journalists' and board members' homes and, most critically, impersonating people to obtain private phone records.

Taking turns, subcommittee members quoted from thick binders of internal documents and reports, and interrogated the panelists on what they knew and whether they still stood by their actions.

Dunn, who has resigned in the scandal, received or authored many of the e-mails. She acknowledged being party to briefings about the investigation but did not accept responsibility for the methods investigators used, saying she relied on guidance from Hunsaker, Baskins and Hurd. Dunn insisted she never approved the use of pretexting, saying, "I was unaware that the fraudulent misrepresentation of identity was a part of the standard arsenal of HP tactics or used in this investigation."

At one point, Rep. Diana DeGette (D-Colo.) said: "Ms. Dunn, you knew that a lot of these techniques were going on. You just didn't think it was your job to do anything about it."

Hurd, facing less confrontational questioning, called the investigators' methods "a rogue investigation that violated our own principles and values." He said he wished he had heeded signs that things were amiss, and added, "It will never happen again."

But subcommittee members said there were plenty of red flags in the case that should have made HP executives aware the company was entering unethical territory. In particular, HP executives approved sending false information to a News.com reporter, which contained an e-mail tracer that they hoped would lead them to the anonymous source quoted in her stories.

DeGette asked Dunn if she was at all concerned about the technique used in an operation to "sting" a reporter to trick her

into revealing her source.

"I sent the team to management to get approval for their techniques," Dunn replied.

"Who was that in management?" DeGette said.

"Mr. Hurd," she said.

For his part, asked whether he knew about the monitoring of board members and their families, the monitoring of reporters and the phone pretexting, Hurd said no each time. He faced the sharpest questioning when it came to the e-mail ruse in which HP investigators made up a fictitious tipster named "Jacob."

DeGette asked Hurd if he thought it was "ethical for investigators to be coming up with a fake individual to be e-mailing reporters."

"Let me try to tell you what was going through my head," he began.

"Yes or no," she said.

Pressed to answer, he shook his head "no."

Dunn stood by her decision to investigate boardroom leaks, restating her position that it was necessary to protect company trade secrets and confidential deliberations. "I believe that these methods may be quite common, not just at Hewlett Packard, but at companies around the country," she said of corporate-sponsored investigations. "Every company of consequence has people who do detective-type work in order to ferret out the sources of nefarious activities." HP launched its effort to flush out who leaked boardroom secrets after a series of news stories appeared in early 2005, citing sources close to its board. Investigators' actions, which members of the subcommittee compared to B-grade movie scripts, have spawned both state and federal criminal probes.

Though most of the questioning was cutting, there were moments of levity.

Rep. Joe Barton (R-Tex.) said stealing phone records was theft. To underscore his point, he asked Dunn whether she would give him her phone records.

"In your position, I would give you my phone records," Dunn said after some hesitation, soliciting laughter from the standing-room only crowd.

"I wouldn't give you mine," Barton retorted.

When a committee member encouraged Hurd to call the House majority leader and endorse legislation outlawing the unauthorized access to phone records, Hurd responded, "You have my support." There are four such bills pending in the House and Senate.

In addition to Hunsaker and Gentilucci, both of whom resigned from HP this week, and Baskin, others pleading the Fifth Amendment yesterday were Ronald DeLia, managing director of outside investigator Security Outsourcing Solutions Inc.; Joseph DePante, owner of Action Research Group; and Bryan Wagner, Charles Kelly, Valerie Preston, Cassandra Selvage, Darren Brost, all private investigators and subcontractors to Action Research Group.

EXHIBIT 12

Business Week Online
September 18, 2006
By Lorraine Woellert
Verizon Caught in HP Pretexting Web

The privacy of Verizon customers' phone records was compromised, putting a top company exec—and Hewlett-Packard board member—in a tough spot

Investigators working on behalf of Hewlett-Packard (HPQ) masqueraded as telecom employees to obtain phone records of Verizon Communications (VZ) customers, BusinessWeek has learned.

Verizon is cooperating with California Attorney General Bill Lockyer, who is investigating methods used by agents working on HP's behalf to uncover the source of company leaks to news outlets.

The victimization of Verizon and its customers puts Verizon Vice-Chairman and President Lawrence T. Babbio in a difficult position. Babbio sits on HP's board and has been a vigorous defender of Chairwoman Patricia Dunn, who launched a controversial probe into corporate leaks to the news media. Babbio has publicly praised Dunn's determination to identify the source of the leaks. Verizon also provides telecom services to Hewlett-Packard.

But as president of Verizon, Babbio has aggressively fought to defend customers from "pretexters," filing civil lawsuits against individuals and cooperating with law enforcement on criminal cases. Eric Rabe, senior vice-president for media relations at Verizon, declined to comment on any facet of the HP investigation. He says Verizon has "zero tolerance" for any intrusion into customer privacy. "We work side by side with law enforcement and certainly would in any case involving pretexting," Rabe says.

SECOND TELECOM AFFECTED. Pretexters—also known in the vernacular as "phone phreakers" or "social engineers"—misrepresent their identities to convince the telecom system to cough up confidential information about phone customers. In the Hewlett-Packard case, tech-savvy gumshoes used Social Security numbers and other information to bluff their way into obtaining the confidential records of phone company customers. Among the individuals targeted were HP directors and employees, plus nine journalists who reported on the company—including three BusinessWeek writers (see BusinessWeek.com, 9/8/06, "BW Writers Targeted by HP").

Several AT&T (T) customers, including former HP board member Thomas Perkins and several journalists, were among the individuals whose records were obtained by pretexters working on Dunn's probe. The revelation that Verizon customers were targeted as well doesn't necessarily mean that the practice was more widespread than HP has acknowledged. AT&T also is cooperating with investigators.

Congressional lawmakers have been studying the pretexting phenomenon for seven months, and now they, too, are putting Hewlett-Packard under their scrutiny. On Sept. 14, a panel of the House Energy and Commerce Committee sent letters asking Dunn and three others to testify before House investigators. Rep. Ed Whitfield (R-Ky.), chairman of the Oversight and Investigations Subcommittee, has scheduled a hearing for Sept. 28.

EXECS CALLED TO TESTIFY. In addition to Dunn, Whitfield has summoned to testify HP Vice-President Ann Baskins; HP outside counsel Larry W. Sonsini, chairman of Wilson Sonsini Goodrich & Rosati; and Ronald DeLia, managing director of Security Outsourcing Solutions, a company linked to the investigation. The subcommittee has asked HP for all documents and correspondence relating to the company's investigation into media leaks. The first set of documents is expected to be delivered on Sept. 18.

HP spokesman Michael Moeller said the company is cooperating with lawmakers but declined to say whether Baskins or Dunn would appear at the hearing. DeLia could not be reached for comment. A spokesman for Sonsini declined to comment.

The Justice Dept. and Securities & Exchange Commission also are looking into Hewlett-Packard's activities after former board member Perkins last month alerted the agencies to Dunn's investigation and the use of pretexting by the company's investigators (see BusinessWeek.com, 9/6/06, "Perkins Goes Up Against HP—Again"). In May, Perkins resigned from the board in protest of Dunn's methods. He went public with his concerns last month. Board member George Keyworth, identified by Dunn as having spoken to the media without going through proper corporate channels, resigned on Sept. 12 and is negotiating a settlement with the company. Dunn will step down from the chairman's seat in January, to be succeeded by CEO and President Mark V. Hurd.

SHAREHOLDER LAWSUIT. The scandal hasn't yet had an effect on the company's stock price, but the first shareholder lawsuit was filed on Sept. 14 by class-action king William S. Lerach, founding partner of Lerach Coughlin Stoia Geller Rudman & Robbins in San Diego. The derivative complaint, filed by shareholder Juliet Worsham in Santa Clara County Superior Court on behalf of the company, accuses Dunn, Baskins, the HP board, and Hurd of "gross mismanagement," breaching fiduciary duty, wasting corporate assets, and abusing control. Faced with numerous federal and state investigations, "HP is unable to protect itself or remedy the wrongs inflicted upon it," the complaint states, because the corporation remains under the control of "the primary wrongdoers" and continues to receive legal advice from Sonsini and Baskins, both of whom have "substantial conflicts of interest" and who also might be implicated in "the commission of the unlawful conduct or covering it up."

The complaint paints HP's board and its "conspirators" as "colossally stupid" and asks the court to impose a host of good-governance practices on the company. Among the shareholder demands are changes in company bylaws that would require HP's chairman to be a non-executive director and permit shareholders to nominate at least three candidates for election to the board. The lawsuit also asks for unspecified punitive damages and legal fees.

Woellert is a correspondent in BusinessWeek's Washington bureau

EXHIBIT 13

NEWS

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

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

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

FOR IMMEDIATE RELEASE
January 17, 2006

NEWS MEDIA CONTACT:
Barry Ohlson: (202) 418-2300
e-mail: barry.ohlson@fcc.gov

STATEMENT BY COMMISSIONER JONATHAN S. ADELSTEIN ON BROKERING OF PERSONAL TELEPHONE RECORDS

I am alarmed by reports that data brokers are obtaining and selling customers' personal telephone records without the customers' consent or knowledge. These records can include some of the most private personal information about an individual. Finding out who people are calling and for how long can be like picking someone's brain about their friends, plans or business dealings. Congress recognized the sensitivity of this information in the Telecommunications Act of 1996 when it prohibited phone companies from using or disclosing certain proprietary customer information without the customer's approval. It charged the FCC with enforcing this privacy protection.

I appreciate the recent efforts of phone companies to take action against these data brokers. Still, the Commission must also take immediate steps to ensure that we have strong consumer privacy rules in place and that phone companies are employing effective safeguards to shield this data from harm. The FCC's Enforcement Bureau has launched an investigation into these troublesome data brokering practices, and I support swift action against carriers that have not complied with our existing rules and procedures. In addition, a petition for rulemaking on enhanced consumer data protection standards filed by the Electronic Privacy Information Center (EPIC) in August 2005 could be an appropriate vehicle for tightening our rules. I support quick action by the Commission to address any abuses of this private information.

- FCC -

EXHIBIT 14

Pretexting the latest identity threat
By Pamela Yip. Monday, Jan. 01, 2007
Dallas Morning News

DALLAS - Identity theft has many facets, and the latest is called "telephone pretexting."

That occurs when someone calls you or a company you do business with and, on a pretext, tries to obtain your personal information.

Pretexting came into the spotlight during the scandal over Hewlett-Packard Co.'s attempts to staunch boardroom leaks. The company acknowledged hiring private investigators to acquire the personal phone records of company directors, journalists and others.

Most people will never be involved in such high-level skullduggery, but everyone needs to be aware of the threat that pretexting poses to their finances and privacy.

Once they get their grubby hands on your personal information, pretexters may sell your data to crooks who may use it to get credit in your name or steal from your bank account.

That's the classic identity theft scenario, in which the criminals don't care who their victim is. But often there are more insidious motives behind pretexting.

The information is frequently used by data brokers, private investigators, loan collectors or individuals involved in private disputes who are looking for specific information about a person.

Federal officials say they don't know how extensive pretexting is.

"We have no way of knowing," said Betsy Broder, an assistant director of the Federal Trade Commission's Division of Privacy and Identity Protection.

The FTC is working with the Federal Communications Commission to investigate and catch pretexters. Both agencies have pursued data brokers who've sold consumers' telephone records.

Federal law already makes it illegal to obtain financial records by pretexting. But no federal law explicitly makes pretexting for phone records unlawful.

The HP case highlighted that gap and put the spotlight on pretexting for telephone records.

You can take steps to protect your information from pretexters.

One piece of advice applies to any fraud protection strategy: Be very wary of people who call you out of the blue, no matter who they say they are.

Don't give out information over the phone, through the mail or over the Internet unless you've initiated the contact or know whom you're dealing with.

"We would strongly advise customers to act with prudence and question heavily any caller who is trying to obtain information about them," said Bill Kula, spokesman for Verizon Communications Inc.

"If a customer receives a call and senses something awry or suspicious, they shouldn't release any information," he said. "Promptly call Verizon, and we can confirm whether we really are trying to speak to one of our customers."

There's another prevention strategy, one that applies directly to pretexting. It involves creating an online account with your telephone company so you can access your billing and call records.

Some people are wary of setting up accounts online, afraid that their information will be stolen. But experts say setting up your account online can actually prevent that from happening because it creates another barrier a potential pretexter must hurdle.

Verizon requires its customer service representatives to check if a customer has established a password on the account before disclosing information, Kula said.

If you've established an online account, "it's one way to make it less likely that someone will get your phone records," Broder said. "That's one way to thwart one type of pretexting."

Before creating online access to their account, customers must have their phone bill in front of them, because they will be asked to supply the customer code or account number from the bill, Kula said.

"Your password is the most important thing that you need to focus on," said Jimmy Duvall, spokesman for Verizon Wireless. "Make sure you have passwords on all your accounts. Don't use obvious passwords, and don't share your password with anyone."

An obvious password might be your mother's maiden name, the last four digits of your Social Security number, your birth date, your phone number or any series of consecutive numbers. The best password is a random string of numbers and letters. Write it down and keep it in a safe place.

Federal regulators are studying what phone companies are doing to protect customer information, what the weaknesses are and what improvements are needed.

"We are investigating the telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers," FCC Chairman Kevin Martin told Congress early this year.

Officials of Verizon and AT&T Inc. have filed lawsuits against those who have obtained customer information under false pretenses.

"We are actively pursuing pretexters in civil courts on potential criminal charges," said Walt Sharp, an AT&T spokesman. "We do take the privacy of that information very seriously."

Like Verizon, AT&T requires customers to provide "very detailed information" before it releases customer information. But Sharp declined to identify what exactly AT&T requires, saying the company doesn't want to give thieves a road map.

The FTC and FCC want Congress to make pretexting for phone records a federal crime, providing them with enhanced enforcement powers. So far, the FTC has had to pursue cases under its mandate to stamp out "unfair and deceptive practices" in commerce.

Several bills that would criminalize pretexting for call histories have been introduced in Congress, but none has come up for a full floor vote.

"Although the acquisition of telephone records does not present the same risk of immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into customers' privacy and could result in stalking, harassment and embarrassment," Joel Winston, associate director of the FTC's Division of Privacy and Identity Protection, told Congress in September.

If you think your customer information has been disclosed without your permission, contact your telephone company right away. Also, file a complaint with the FCC at www.fcc.gov/cgb/complaints.html, or call 1-888-225-5322 (toll free). But remember that there's no guarantee that you'll escape the clutches of pretexters.

"Pretexters are very resourceful," Broder said. "Even if a consumer takes all the precautions, it doesn't necessarily ensure that their records won't be accessible by some fraudsters."

EXHIBIT 15

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.

2

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

EXHIBIT 16

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

Tuesday , May 16, 2006

Associated Press

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

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

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

• Click here to read the USA Today article.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EXHIBIT 17

Excerpts from Verizon's Privacy Policies

http://www22.verizon.com/about/privacy/customer/

However, we do release customer information without involving you if disclosure is required by law or to protect the safety of customers, employees or property.

When you dial 911, information about your location may be transmitted automatically to a public safety agency.

Verizon must disclose information, as necessary, to comply with court orders or subpoenas. Verizon
also will share information to protect its rights or property and to protect users of its services and other carriers from fraudulent, abusive or unlawful use of services.

We may, where permitted by law, provide information to credit bureaus, or provide information and/or
sell receivables to collection agencies, to obtain payment for Verizon billed products and services.

http://www22.verizon.com/about/privacy/genpriv/

Principle 9:
Verizon complies with all applicable privacy laws and regulations wherever Verizon does business.

Customer and policymaker perceptions of privacy have changed over time and will continue to do so. Changes in technology can also alter what is appropriate in protecting privacy. Laws may change accordingly. We will regularly examine -- and update, if necessary -- the Verizon Privacy Principles.

Not only will Verizon comply with all applicable privacy laws, but we'll carefully monitor customer needs and expectations. And Verizon will work with policymakers and consumers to ensure that we continue to safeguard privacy, giving customers choices, flexibility and control.

Verizon considers privacy laws and regulations to be the minimum standards we will adhere to in protecting privacy. In addition to complying with the law, Verizon will also adhere to these Privacy Principles wherever we do business.

http://www.verizonwireless.com/b2c/globalText?contentType=globalContent&jspName=footer/privacyPrinciples.jsp&textName=PRIVACY_POLICY

An example of when we would disclose personally identifiable information to an outside person or entity is when we are served with a subpoena for customer information. In such cases, we are required to release the information. Another example would be if we share personally identifiable information with other carriers and/or with law enforcement to prevent and investigate fraud and other unlawful use of communications services.

We support notice and informed consent for the use of any personally identifiable wireless

location and transactional information. We will not store this type of information beyond its normal useful life, including for internal service evaluation and quality assurance purposes, except as required by law.

Compliance With Laws and Public Policy Participation

- **We support consumer, government and industry efforts to identify and resolve privacy issues.**

  We participate in legislative and regulatory proceedings, industry association efforts, consumer group efforts and general business group activities relating to telecommunications privacy issues.

- **We comply with all applicable privacy laws and regulations wherever we do business.**

  Customer and policymaker perceptions of privacy have changed over time and will continue to do so. Changes in technology can also alter what is appropriate in protecting privacy. Laws may change accordingly. We will regularly examine - and update, if necessary - these Principles.

  We consider privacy laws and regulations to be the minimum standards we adhere to in protecting privacy. In addition to complying with these laws and regulations, we also adhere to these Principles wherever we do business.

  We also have taken additional voluntary measures to affirm our commitment to safeguarding your privacy. For example, we adhere to the CTIA Consumer Code for Wireless Service, we are a licensee of the TRUSTe Website Privacy Program and our web site meets the BBB*OnLine*'s Reliability Program Standards.

- **We comply with all applicable laws and regulations regarding 'spam' and use commercially reasonable efforts to combat wireless 'spam'.**

  We supported the passage of federal legislation aimed at providing consumers with control over receipt of unsolicited electronic messages, or 'spam'. We employ tools in our network to detect incidences of 'spam' sent to our customers' wireless devices, and we also provide customers with tools to manage and even restrict receipt of such messages. We may take legal action against 'spammers' who abuse our network.

We do not tamper with, intrude upon or intentionally disclose the existence or contents of any communication or transmission, except as required by law or the proper management of our network, or with your consent.

http://www.verizonwireless.com/b2c/footer/accountSecurity.jsp?action=view&item=popup

Account Security

You may be aware of recent events and news stories concerning "pretexting," the fraudulent, deceitful or otherwise illegal attempts by unscrupulous individuals to gain access to account information of phone customers. Be assured that the security of your personal information continues to be one of the highest priorities at Verizon Wireless. We have taken aggressive steps to identify and sue individuals employing these deceitful tactics, and we will not let up.

There are several affirmative steps that you can take to help protect against unauthorized access to your Verizon Wireless account information by pretexters. For example:

* You can establish a user name and password restricting unauthorized access to your online account by visiting www.verizonwireless.com. This only takes a few moments and is one of the best ways to prevent others from establishing an online account in your name (so as to view your account information). Pick a password that is not obvious and keep it secret.

* If you have already established an online account and are concerned that someone may know or guess your user name and password, consider changing your login information for your online account.

* You can also prevent someone who is trying to impersonate you when calling our customer service representatives from accessing your personal information by establishing a four-digit billing system password. You can create this password by contacting our customer service representatives.

* Always keep personal information such as account numbers, social security numbers and passwords in secure places, and do not share this information with others.

www.verizononline.net

Do you sell or give my information to non-Verizon companies, other third parties or governmental entities?

Verizon does not sell or disclose individually-identifiable information obtained online, or information about you or your account or service, to anyone outside of Verizon or its authorized vendors, contractors and agents unless you specifically authorize it, disclosure is required by law, or deemed necessary by Verizon in its sole discretion to protect the safety, rights or property of Verizon or any other person or entity. If you provide individually identifiable information to us in the context of an event Verizon sponsors with another company, such as a contest, or if you register on a co-sponsored site or feature, you may also be providing the individually identifiable information to the co-sponsor. For example, on Verizon co-branded sites, our partner will generally co-own the customer information received through the site. How the partner uses this information will be explained in the privacy statement at the co-branded site, which will govern the use of data gathered through the co-branded site.

Verizon may share non-personally identifiable information with non-Verizon companies in order to assess the results of a promotion or event. This information is used in aggregate only, and does not contain any information that would personally identify you.

How does Verizon prevent unauthorized access to my information?

Your password is set at a minimum of six characters, which provides added protection for your personal information. On secured pages, this site uses SSL encryption up to 128-bits.

Information that you share about yourself in chat rooms, message boards, instant messaging communications and similar forums becomes immediately available to others who have access to those fora. These areas are considered public spaces and Verizon Online cannot protect the privacy of information disclosed therein. Please exercise caution when disclosing personal information in theses areas.

Mary Louise Weber
Assistant General Counsel

Verizon Communications Inc.
One Verizon Way, Rm VC54S440
Basking Ridge, New Jersey 07920
Phone 908 559-5636
Fax 908 696-2068
mary.l.weber@verizon.com

February 5, 2007

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

Re: Verizon Communications Inc. 2007 Annual Meeting
Shareholder Proposal of Thomas Van Dyck

Ladies and Gentlemen:

I refer to my letter dated December 27, 2006 (the "December 27 Letter") pursuant to which Verizon Communications Inc., a Delaware corporation ("Verizon"), requested that the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission concur with Verizon's view that the shareholder proposal and supporting statement (collectively, the "Proposal") submitted by Thomas Van Dyck (the "Proponent") may properly be omitted pursuant to Rule 14a-8(i)(7), Rule 14a-8(i)(2), Rule 14a-8(i)(10), and Rule 14a-8(i)(3) and Rule 14a-8(i)(6) from the proxy materials (the "Proxy Materials") to be distributed by Verizon in connection with its 2007 annual meeting of shareholders.

This letter is in response to the letter to the Staff by the Proponent's counsel, dated January 23, 2007 (the "Proponent's Response Letter"), and supplements the December 27 Letter. In accordance with Rule 14a-8(j), a copy of this letter is being sent simultaneously to the Proponent and his counsel.

I. Overview.

The Proponent's Response Letter purports to refute the numerous authorities cited by Verizon in the December 27 Letter that support exclusion of the Proposal from its Proxy Materials by asserting, in effect, "No, the report being requested is not about that." If the Proponent's position is to be taken at face value, the requested report would have very little, if anything, to do with Verizon, its business operations or its customers, but instead would be in the nature of a graduate student's doctoral thesis or a government "white paper" on "the overarching technological, legal and ethical policy issues" involving rights to privacy. While such a report may be of interest to the

Proponent, it is a misuse of the Rule 14a-8 process to place the burden of researching and preparing such a report on Verizon.

According to the Proponent, the requested report does not concern the ordinary business matters of protecting customer information, complying with law enforcement requests and other legal requirements, determining litigation strategy or evaluating the effects of political or legislative proposals on Verizon's business operations, simply because it is not about those things. It "avoids this pitfall by focusing on the 'overarching technological, legal and ethical policy issues.'" [Proponent's Response Letter page 9].

In the same vein, the Proponent claims the requested report would not require Verizon to violate one or more federal laws or defy the instructions of the United States Justice Department concerning the treatment of classified information, because it is not about those things; i.e., "the *details* of an intelligence program" or Verizon's alleged involvement. Because "the Proposal has struck the appropriate balance by avoiding being too general or too specific," the requested report is only *hypothetically* about those things. [Proponent's Response Letter page 16]

Likewise, the Proponent asserts that Verizon has not substantially implemented the Proposal by posting extensive materials about its privacy policy and principles on it website, because it is not about those things. Even though the plain language of the Proposal calls for a report that "describes" the issues, the Proponent claims that the Proposal requests "a *discussion* and that implicitly calls for a presentation of differing ideas and approaches." (Proponent's Response Letter page 18]

The thrust of the Proponent's Response Letter is that the Proposal requests a general, open-ended discussion of "overarching" issues that affect privacy rights. But, if that is the case, the requested report is so inherently vague and indefinite that it runs afoul of Rule 14a-8(i)(3) and Rule 14a-8(i)(6). Indeed, it is evident that the Proponent recognizes this substantial defect in the Proposal, because the Proponent attempts to address the defect by insisting repeatedly, *without support or justification*, that the Proposal "has struck the proper balance between specificity and generality."

The Proponent's bare statement that the Proposal has struck the "proper balance" does not make it so and cannot overcome the inherent defects of the Proposal; namely that it either (1) deals with ordinary business matters or matters the disclosure of which would violate federal law or (2) is so open-ended and wide-ranging that it would be impossible for either the shareholders voting on the Proposal or Verizon in implementing it "to determine with any reasonable certainty exactly what actions or measures the proposal requires." [Staff Legal Bulletin No. 14B (September 15, 2004) discussing when a proposal violates Rule 14a-8(i)(3)]

II. The Proponent Incorrectly Asserts That Reports Which Are "Overarching" in Nature and Provide for a General Discussion of "Policy Issues" Cannot Violate Rule 14a-8(i)(7)

Section I of the Proponent's Response Letter presents a lengthy argument (pages 4 through 14) that the Proposal is not excludable under Rule 14a-8(i)(7). That argument rests heavily on the unique and unsupportable proposition that, because the report requested in the Proposal is (a) intended to be "overarching" in nature, (b) intended to address only general matters of "policy," and (c) not intended to address any particular aspect of Verizon's business, the Proposal cannot be excluded as relating to Verizon's ordinary business operations.

As discussed in Section II.A. of the December 27 Letter, the Staff has long recognized that proposals which attempt to govern business conduct involving internal operating policies, customer relations and legal compliance programs are excludable under Rule 14a-8(i)(7). The Proposal, on its face, undeniably relates to the day-to-day management functions of developing and implementing policies and procedures surrounding the protection of customer information and the circumstances under which that information may be lawfully disclosed. This defect cannot be cured by the Proponent's efforts to describe the report as "overarching" and thus claim that it "transcends the day to day affairs" of Verizon and involves significant social policy issues. A report that pertains to Verizon and its protection of customer information is not a significant social policy issue. It is a report relating to Verizon's ordinary business operations.

In Section I.C. on page 11 of the Proponent's Response Letter, the Proponent attempts to refute Verizon's argument that the Proposal is excludable under Rule 14a-8(i)(7) because it could interfere with Verizon's litigation strategy with respect to ongoing lawsuits by setting up a convenient "straw man." With scant support or justification, Proponent claims that the Proposal is only excludable if it explicitly seeks to dictate the results of the litigation. The Proponent then asserts that this standard is not applicable to the Proposal because "our Proposal requests an overarching policy discussion of the issues surrounding privacy rights and does not request the Company come to any particular conclusion regarding those rights and does not seek thereby to dictate the results of the lawsuits." Given the Proposal's request for, among other things, a report on the legal issues surrounding the disclosure of customer information to governmental agencies without a warrant or to individuals who engage in the unlawful activity of pre-texting, it is difficult to understand Proponent's position that the Proposal does not implicate Verizon's litigation strategy.

In Section I.D. on pages 13-14 of the Proponent's Response Letter, the Proponent seeks to address Verizon's argument, supported by substantial authority on pages 6-7 of the December 27 Letter, that the Proposal inappropriately seeks to engage Verizon in the political or legislative process relating to aspects of Verizon's ordinary business operations. Again, the Proponent seeks to dismiss such authority by claiming the Proposal does not relate "expressly or implicitly, [to] specific legislative or regulatory proposals" (page 13) but instead "seeks a discussion of the issues without a predetermined finding let alone a predetermined legislative result." (page 14).

The Proponent's "predetermined legislative result" argument finds no support in the cited authorities; it is a standard manufactured by the Proponent for purposes of his argument. Not only does the Proponent fail to refute Verizon's authorities relating to political or legislative aspects of his Proposal, but he unintentionally supports Verizon's position with the numerous references, on page 7 of the Proponent's Response Letter, to Gallup Poll results, media reports, Congressional interest, a quote from a Senator and state regulatory issues. Given the nature of the entire Proponent's Response Letter, it is difficult to understand the Proponent's argument that the Proposal does not seek to involve Verizon in the political or legislative process.

Finally, it should be noted that, after an ineffectual attempt to cast the issue of pretexting as a significant social policy issue on page 8, the Proponent's Response Letter conveniently neglects the subject for the remainder of the letter. This is understandable, because it is virtually impossible to construct a plausible argument that pretexting is anything more than an ordinary business matter for a telecommunications company. A person or entity that engages in pretexting commits a fraudulent and illegal act. The development of policies, procedures and technology to combat that fraudulent act, and the consideration of the legal issues surrounding it, are clearly ordinary business activities within the scope of Rule 14a-8(i)(7). As indicated on page 8 of the December 27 Letter, the no-action precedent under Rule 14a-8(i)(7) supports the exclusion of a proposal in its entirety where only part of the proposal relates to ordinary business matters. Thus, even if the Staff were to agree with the Proponent's position that one part of the Proposal focuses on matters that transcend the day-to-day operations of Verizon, the Proposal nonetheless is excludable under Rule 14a-8(i)(7) because the other part of the Proposal clearly focuses on ordinary business matters.

III. The Proponent Mischaracterizes Verizon's Argument That The Proposal Is Excludable Under Rule 14a-8(i)(2)

The Proponent's argument, in Section II of the Proponent's Response Letter at pages 14 through 17, regarding the violation of federal law exclusion under Rule 14a-8(i)(2), does not address the fundamental aspect of Verizon's argument on the subject, as set forth in Section II.B. of the December 27 Letter, and as supported by an opinion of Verizon's counsel which accompanied the December 27 Letter. Verizon's

fundamental argument is that the United States has expressly and formally advised it on several occasions that Verizon would violate federal law if it were to disclose classified information it may possess concerning intelligence-gathering activities allegedly carried out by the federal government, at the direction of the President of the United States, as part of the government's post-September 11 program to prevent terrorist attacks.

Instead, the Proponent, at various points, argues that classified or other prohibited information would not be included in the requested report; refers to a case relating to AT&T (and not to Verizon); and refers to a "state secret privilege," which is not the basis for Verizon's argument for exclusion. As indicated in Attachment A hereto, Verizon's counsel has reviewed the Proponent's Response Letter and confirmed that nothing in the Proponent's Response Letter affects it original opinion. The Proponent also seemingly argues that there would be no violation of federal law "because the Proposal has struck the appropriate balance by avoiding being too general or too specific." The Proponent even goes as far as to suggest, on page 16, that the report could avoid violating federal law by being prepared on the basis of hypothetical facts, with some type of caveat that, for purposes of the report, Verizon "accept[s] at face value all the facts asserted in the media reports." There is nothing in Rule 14a-8(i)(2) that requires a company to attempt to evade a direct warning from the United States government that disclosure of certain information is illegal, by disclosing that information on a hypothetical basis.

IV. The Proponent Incorrectly Argues That Verizon Has Not Substantially Implemented the Proposal Because the Proposal Is "Overarching" In Nature

In a familiar refrain, the Proponent asserts in Section III of the Proponent's Response Letter on page 18, that the disclosures on Verizon's website, as discussed in Section II.C. of the December 27 Letter, do not constitute substantial implementation of the Proposal because such website disclosures are "far removed from a discussion of 'the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content...'"

In addition, the Proponent argues, also on page 18, that Verizon's websites are "intended to communicate information to *customers* while the Proposal requests information for *shareholders*," and that Verizon's websites "do not present the information in the same form as we request." These arguments are not validly supported or persuasive, nor are they relevant to application of Rule 14a-8(i)(10).

V. The Proponent's Response Letter Supports Verizon's Argument That the Proposal Is Inherently Vague and Indefinite and, Therefore, False and Misleading

As discussed in detail above, the Proponent's response to virtually every cited basis for exclusion of the Proposal is, *in effect*, that such exclusion is inapplicable because of the "overarching" nature of the requested report. Such an overarching report, which the Proponent suggests could even be prepared on a hypothetical basis, is, as stated above, more in the nature of a graduate student's doctoral thesis or a government "white paper" than a corporate report to shareholders. As discussed in Section II.D. of the December 27 Letter, the contemplated report is vague and indefinite and, therefore, false, misleading, and excludable under Rule 14a-8(i)(3) and Rule 14a-8(i)(6).

The Proponent evidently recognizes this substantial defect in the Proposal, and seeks to remedy the defect by repeatedly asserting, without support or justification, that the Proposal strikes just the right balance between specificity and generality. For example:

- "...we believe the Proposal has struck the right balance between specificity and generality." (page 2)
- "the Proposal strikes the appropriate balance by focusing on the policy level issues while providing sufficient guidance so that the shareholders and management understand what is being requested." (page 9)
- "the Proposal has struck the appropriate balance by avoiding being too general and too specific." (page 15)
- "the proposal has struck the proper balance between specificity and generality..." (Caption of Section IV on page 19)

In fact, the Proposal strikes no such proper balance. *In an effort* to sidestep the substantive requirements of Rule 14a-8, the Proponent has defined the requested report as one which has little, if anything, to do with Verizon or its business, and is simply a dissertation on subjects of interest to the Proponent. This renders the Proposal vague and indefinite and, therefore, false and misleading, and excludable

under Rule 14a-8(i)(3) and Rule 14a-8(i)(6). The Proponent's "proper balance" arguments do not overcome the inherent defects in the Proposal.

VI. Conclusion

Despite the Proponent's attempt to navigate around the numerous authorities that support exclusion of the proposal by stressing the "overarching" nature of the requested report, the Proponent cannot "avoid the pitfall" presented by the incontrovertible fact that the subject of the Proposal – customer privacy rights – is not only a matter of a complex nature, but one that is absolutely fundamental to Verizon's day to day business operations. At the conclusion of the Proponent's Response Letter, the Proponent inadvertently highlights the defects of the Proposal by offering alternative examples of how Verizon could approach the report. The Proponent suggests as one possibility that Verizon could discuss "the feasibility of [Verizon] contributing to technological advancements which would allow the company to assist law enforcement more effectively" while protecting customer privacy, as well as "report on technological advancements that cut down on pretexting." [Proponent's Response Letter page 21] Such a report would clearly fall within the scope of the Rule 14a-8(i)(7) exclusion, as seeking to micro-manage the company. Assessing the feasibility and benefits of new technologies for use in business operations is clearly an ordinary business matter. Moreover, information of this nature is generally considered to be confidential and proprietary. As another possibility, the Proponent identifies a number of laws that are applicable to Verizon and suggests that the report could discuss the "business implications" of these laws. Again, analyzing the impact of various laws on Verizon's business clearly falls within the scope of the Rule 14a-8(i)(7), as seeking to micro-manage the company. Moreover, it is likely that the requested discussion (which the Proponent asserts should present differing positions) could compromise Verizon's positions in pending lawsuits and regulatory proceedings.

For the reasons set forth above and in the December 27 Letter, Verizon continues to believe that the Proposal may properly be omitted from the Proxy Materials pursuant to Rule 14a-8(i)(7), Rule 14a-8(i)(2), Rule 14a-8(i)(10), and Rule 14a-8(i)(3) and Rule 14a-8(i)(6), and requests the Staff's concurrence with its views.

Kindly acknowledge receipt of this letter by stamping and returning the extra enclosed copy of this letter in the enclosed self-addressed, stamped envelope. If you have any questions with respect to this matter, please telephone me at (908) 559-5636.

Very truly yours,

Mary Louise Weber
Assistant General Counsel

cc: As You Sow Foundation
311 California Street, Suite 510
San Francisco, CA 94104

Jonas D. Kron, Esq.
P.O. Box 42093
Portland, Oregon 97242

EXHIBIT "A"

WILMERHALE

John A. Rogovin

+1 202 663 6270 (t)
+1 202 663 6363 (f)
john rogovin@wilmerhale.com

February 5, 2007

Board of Directors
Verizon Communications Inc.
c/o Mr. William P. Barr
General Counsel
One Verizon Way
Fourth Floor
Basking Ridge, New Jersey 07920

Re: Shareholder Proposal

Dear Members of the Board:

You previously requested that we, as special counsel to Verizon Communications Inc. ("Verizon") in litigation and related proceedings concerning Verizon's alleged involvement in certain intelligence-gathering programs of the federal government, provide our legal opinion on a shareholder proposal submitted by Mr. Thomas Van Dyck (the "Proposal") to Verizon for inclusion in its 2007 proxy statement. In a letter dated December 27, 2006 (the "Opinion Letter"), we concluded that implementation of the Proposal would violate one or more federal laws to which Verizon is subject. You have now requested that we review our conclusions in light of a letter submitted on January 23, 2007, by Mr. Jonas D. Kron (the "Kron Letter") to the Securities and Exchange Commission regarding the Proposal.

Subject to the provisions, conditions, and limitations contained in our Opinion Letter—which we hereby incorporate by reference—nothing in the Kron Letter affects the conclusions set forth in our Opinion Letter.

Very truly yours,

WILMER CUTLER PICKERING
HALE AND DORR LLP

By: _____
John A. Rogovin, a Partner

JONAS D. KRON, ATTORNEY AT LAW

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

February 8, 2007

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

Re: Shareholder Proposal of Thomas Van Dyck Submitted to Verizon Communications Inc. for inclusion in its 2007 Proxy materials.

Dear Sir/Madam:

On behalf of Verizon shareholder Thomas Van Dyck ("Proponent") this letter is a response to Verizon's ("the Company") second letter on this matter, dated February 5, 2007. Pursuant to Rule 14a-8(k), enclosed are six copies of this letter. A copy of this letter is being mailed concurrently to Verizon's Assistant General Counsel Mary Louise Weber.

While the Company makes a strenuous attempt to bolster its original contentions and confuse matters with rhetoric, we continue to stand by our January 23, 2007 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. Because of the spurious nature of many of Verizon's statements and the lack of any reasoned legal analysis it is not necessary to respond to each and every point raised in the Company's protracted February 5th letter.

Despite all of the verbiage found in Verizon's letter the questions before the Staff essentially boil down to whether the Company has met its burden of demonstrating that it is entitled to exclude the Proposal because:

1. the Proposal does not involve any substantial policy or other considerations;
2. decided legal authority establishes that implementation would violate the law;
3. Verizon has substantially implemented the Proposal; and
4. the Proposal is so vague that it would be impossible to implement.

Taking each of these questions in turn the answer is clearly no, the Company has not met its burden.

I. Rule 14a-8(i)(7) - Significant Policy Issue.

Under well established authority of the Securities and Exchange Commission and the courts it is abundantly clear

> that **all proposals could be seen as involving some aspect of day-to-day business operations.** That recognition underlies 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.**

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). Despite page after page of non-legal argument in the Company's February 5th letter, this essential and basic principle enunciated by the Securities and Exchange Commission and the courts goes undisputed.

Furthermore, it is beyond argument that we have provided the Staff with extensive documentation demonstrating how consumer privacy rights are a significant policy issue that transcends the day-to-day affairs of the Company. (Please see pages 7 and 8 of our January 23rd letter). In contrast, Verizon has done essentially nothing to disabuse anyone of the conclusion that it is a significant policy issue. For all intents and purposes they have conceded that it is a significant policy issue. As such, they have not met their burden of demonstrating that they are entitled to exclude the Proposal under Rule 14a-8(i)(7).

II. Rule 14a-8(i)(2) – Violation of the Law.

In Section III of its February 5th letter, the Company states that its "fundamental argument is that the United States has expressly and formally advised it on several occasions that Verizon would violate federal law if it were to disclose classified information . . ." That, however, misses the point of Rule 14a-8(i)(2) which requires that the company point to "compelling state law precedent" or "decided legal authority." *The Quaker Oats Company* (April 6, 1999). With all due respect to the United States Attorney General and Director of National Intelligence, referred to by the Company as authority, their opinions do not constitute compelling legal precedent or decided legal authority. In fact, *The Hon. Judge Vaugh R. Walker's July 20, 2006 Order in Hepting v. AT&T Corporation*, which we discussed at length at pages 16 and 17 of our January 23rd letter, clearly demonstrates that the issue is far from decided and that there is no compelling legal precedent yet established.

Finally, we note that on page 5 of its February 5th letter Verizon faults us for referring to the AT&T case and the state secrets privilege. However, we observe that the WilmerHale letter at page 4 refers to

the exact same AT&T litigation and state secrets privilege to make the Company's argument. We suggest that what is good for the goose is good for the gander and that Verizon's argument be disregarded out of hand.

III. Rule 14a-8(i)(10) – Substantial Implementation.

The Company, in Section IV of its February 5th letter, essentially responds to our compelling reasoning and extensive citation to analogous cases by making an unsupported assertion that our arguments are not valid, persuasive or relevant. They do not provide us or the Staff with any discussion, reasoning or analysis that could shed some light on the basis for such objections. Furthermore, they do not challenge any of the cases we have cited. Consequently, it is impossible and ultimately unnecessary to respond to these bald assertions and we respectfully refer the Staff to Section III of our January 23rd letter for our analysis of this question.

IV. Rules 14a-8(i)(3), 14a-8(i)(6) and 14a-9 – Vagueness.

As discussed in Section IV of our January 23rd letter, vagueness determinations can become very fact-intensive determination and the Staff has expressed concern about becoming overly involved in such determinations. Staff Legal Bulletin 14B. We stand firmly by our analysis in our January 23rd letter and suggest that the Company has underestimated the importance of privacy issues and the ability of its shareholders to understand the plain meaning of the Proposal. Leaving aside all of the Company's rhetoric, if one simply reads the Proposal it is clear that the Company has not met its burden of demonstrating 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 exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (September 15, 2004).

> RESOLVED: The 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 overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content to (1) the Federal Bureau of Investigation, NSA and other government agencies without a warrant and (2) non-governmental entities (e.g. private investigators) and their effect on the privacy rights of Verizon's MCI long-distance customers.

The Proposal speaks for itself with clarity. We are asking for a description of the customer privacy rights policy issues that are currently confronting the Company – nothing more, nothing less. Despite vigorous attempts to plant seeds of confusion, Verizon has not demonstrated how this is inherently vague or indefinite. As a plain reading of the Proposal demonstrates, it raises the subject of privacy rights clearly and succinctly.

Conclusion

For the reasons given above and in our more extensive letter of January 23, 2007 the Proponent, with all respect, request that the Staff inform the Company that SEC proxy rules require denial of Verizon's no-action request. Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information.

Thank you for your consideration of this matter.

Sincerely,

Jonas Kron
Attorney at Law

cc: Mary Louise Weber, Assistant General Counsel, Legal Department, Verizon
As You Sow Senior Staff
As You Sow Board of Directors
Thomas Van Dyck

Mary Louise Weber
Assistant General Counsel

Verizon Communications Inc.
One Verizon Way, Rm VC54S440
Basking Ridge, New Jersey 07920
Phone 908 559-5636
Fax 908 696-2068
mary.l.weber@verizon.com

February 12, 2007

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

Re: Verizon Communications Inc. 2007 Annual Meeting
Shareholder Proposal of Thomas Van Dyck

Ladies and Gentlemen:

I refer to my letters dated December 27, 2006 (the "December 27 Letter") and February 5, 2007 (the "February 5 Letter"), pursuant to which Verizon Communications Inc., a Delaware corporation ("Verizon"), requested that the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission concur with Verizon's view that the shareholder proposal and supporting statement (collectively, the "Proposal") submitted by Thomas Van Dyck (the "Proponent") may properly be omitted pursuant to Rule 14a-8(i)(7), Rule 14a-8(i)(2), Rule 14a-8(i)(10), and Rule 14a-8(i)(3) and Rule 14a-8(i)(6) from the proxy materials (the "Proxy Materials") to be distributed by Verizon in connection with its 2007 annual meeting of shareholders. In accordance with Rule 14a-8(j), a copy of this letter is being sent simultaneously to the Proponent and his counsel.

This letter briefly responds to certain statements in the letter to the Staff by the Proponent's counsel dated February 8, 2007 (the "Second Response Letter"), as follows:

1. The Second Response Letter, on page 1, asserts that the February 5 Letter "lack[ed]...any reasoned legal analysis." The December 27 Letter contained extensive legal analysis in support of each of Verizon's arguments. This legal analysis was not reiterated in the February 5 Letter; the purpose of the February 5 Letter was to respond to the 24-page letter dated January 24, 2007 from the Proponent's counsel to the Staff (the "First Response Letter").

2. In Section I of the Second Response Letter, the Proponent asserts: "For all intents and purposes [Verizon has] conceded that [the Proposal] is a

significant policy issue." This assertion – perhaps the product of wishful thinking – is incorrect. Verizon respectfully refers the Staff to its detailed and supported arguments in Section II.A. on pages 3-7 of the December 27 Letter, and Section II on pages 3-4 of the February 5 Letter (wherein it is stated, on page 3, "A report that pertains to Verizon and its protection of customer information is not a significant social policy issue. It is a report relating to Verizon's ordinary business operations").

3. Section II of the Second Response Letter advances the illogical argument that there is no basis for exclusion of a proposal under Rule 14a-8(i)(2) on the basis of violation of a criminal law unless and until a violation previously has occurred and one or more persons or entities have suffered a felony conviction. Only then, the Proponent asserts, would there be established "compelling legal precedent" or "decided legal authority." The Second Response Letter does not challenge or refute Verizon's fundamental argument that "the United States has expressly and formally advised [Verizon] on several occasions that Verizon would violate federal law if it were to disclose classified information it may possess concerning intelligence-gathering activities allegedly carried out by the federal government, at the direction of the President of the United States, as part of the government's post-September 11 program to prevent terrorist attacks." (February 5 Letter, Section III, pages 4-5) Instead, the Second Response Letter dismissively states: "With all due respect to the Attorney General and Director of National Intelligence, ... their opinions do not constitute compelling legal precedent or decided legal authority." Verizon disagrees, and reiterates that there is no basis in Rule 14a-8(i)(2) for the Proponent's position that there must have been a commission of a felony and a subsequent criminal conviction before reliance can be placed on Rule 14a-8(i)(2).

4. As discussed in detail in the February 5 Letter, in the First Response Letter the Proponent consistently stated that the Proposal seeks to have Verizon produce a report that is "overarching" in nature, is intended to address only general matters of "policy" and is not intended to address any particular aspect of Verizon's business. For example, in Section III on page 18 of the First Response Letter, the Proponent argued that disclosures on Verizon's website do not constitute "substantial implementation" of the Proposal because such website disclosures are "far removed from a discussion of the overarching technological, legal and ethical policy issues" sought in the report contemplated by the Proposal.

   In Section V on pages 6-7 of the February 5 Letter, Verizon argued that the Proposal is inherently vague and indefinite and, therefore, false and misleading, and excludable under Rule 14a-8(i)(3) and Rule 14a-8(i)(6).

Verizon noted that the Proponent's only response was to assert repeatedly, without support or justification, that the Proposal strikes just the right balance between specificity and generality.

In the Second Response Letter, in an apparent acknowledgement of the fact that the Proposal is vague and indefinite and, therefore, false and misleading, the Proponent describes the Proposal in very different terms. The Proposal, the Proponent now asserts, is a model of "clarity" that asks for "a description of customer privacy rights policy issues that are now confronting [Verizon] – nothing more, nothing less." When the Proponent responds to Verizon's "ordinary business" (Rule 14a-8(i)(7)) and "substantial implementation" (Rule 14a-8(i)(10)) arguments, the Proposal is described as overarching, philosophical and perhaps even hypothical. When the Proponent responds to Verizon's "vague and indefinite" arguments (Rules 14a-8(i)(3) and 14a-8 (i)(6)), the Proposal suddenly is transformed into a clear request for Verizon's customer privacy rights policy.

With these conflicting interpretations of the Proposal advanced by the Proponent himself, it is precisely the type of proposal envisioned by the Staff in Staff Legal Bulletin 14B (September 15, 2004), wherein the Staff stated that a proposal will violate Rule 14a-8(i)(3) when "the resolution contained in the proposal is so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company implementing the proposal (if adopted) would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." Here, even the Proponent has very differing interpretations of his Proposal.

For the reasons set forth above and in the December 27 Letter and the February 5 Letter, Verizon continues to believe that the Proposal may properly be omitted from the Proxy Materials pursuant to Rule 14a-8(i)(7), Rule 14a-8(i)(2), Rule 14a-8(i)(10), and Rule 14a-8(i)(3) and Rule 14a-8(i)(6), and requests the Staff's concurrence with its views.

Kindly acknowledge receipt of this letter by stamping and returning the extra enclosed copy of this letter in the enclosed self-addressed, stamped envelope. If you have any questions with respect to this matter, please telephone me at (908) 559-5636.

Very truly yours,

Mary Louise Weber

Mary Louise Weber
Assistant General Counsel

cc: As You Sow Foundation
311 California Street, Suite 510
San Francisco, CA 94104

Jonas D. Kron, Esq.
P.O. Box 42093
Portland, Oregon 97242

JONAS D. KRON, ATTORNEY AT LAW

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

February 14, 2007

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

Re: Shareholder Proposal of Thomas Van Dyck Submitted to Verizon Communications Inc. for inclusion in its 2007 Proxy materials.

Dear Sir/Madam:

On behalf of Verizon shareholder Thomas Van Dyck ("Proponent") this letter is a response to Verizon's ("the Company") third letter on this matter, dated February 12, 2007. Pursuant to Rule 14a-8(k), enclosed are six copies of this letter. A copy of this letter is being mailed concurrently to Verizon's Assistant General Counsel Mary Louise Weber.

In short, we respectfully disagree with the arguments and conclusions found in Verizon's February 12th letter and believe that there is nothing therein that would lead the Staff to conclude that the Company has met its significant burden of demonstrating that it is entitled to exclude the Proposal from its 2007 proxy materials. Accordingly, we request the Staff refer to our letters of January 23, 2007 and February 8, 2007 for our full analysis of these matters.

It is necessary, however, to respond to two items found in the Company's February 12th letter. First, on page 2 Verizon asserts that we somehow have interpreted *The Quaker Oats Company* (April 6, 1999) to mean that exclusion can only occur in a criminal law context "unless and until a violation previously has occurred and one or more persons or entities have suffered a felony conviction." There is nothing in our letters that even remotely approximates such an interpretation. *Quaker Oats* stands for the simple proposition that the Staff has interpreted Rule 14a-8(i)(2) to require a "compelling state law precedent" or "decided legal authority". We have pointed out that the current status of *Hepting v. AT&T Corporation* means that there is currently no "compelling precedent" or "decided legal authority" to support the Company's position. How Verizon gets from that analysis to a discussion of convictions is not at all evident. Finally, we note that the Company no longer appears to dispute the relevance of *Hepting v. AT&T.*

Second, under number 4 of its February 12th letter the Company has taken our separate vagueness and ordinary business analyses and has tried to rearrange our arguments and words to confuse matters. It is clear that the micro-management exclusion and the vagueness exclusion present two poles on the spectrum of permissible proposals. To pass muster, a proposal can be neither too detailed nor can it be too vague. All shareholders who submit proposals must place their proposals within that spectrum and we have been very cognizant of those requirements. In view of the entirety of the facts and circumstances, as presented in detail in our previous two letters, we believe that we have struck a reasoned and appropriate balance, as the Rule demands. The Company, has tried to confuse this straightforward analysis by picking and choosing words from various parts of our letters and applying them out of context. Our Proposal, as required by the Rule, is specific enough to avoid being vague and it is general enough to avoid the micro-managing exclusion. We respectfully request the Staff concur with this conclusion.

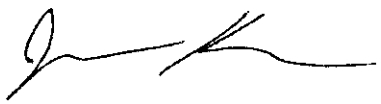
Finally, we note that the Company has not taken this opportunity to challenge the analysis of the ordinary business exclusion we presented in our February 8, 2007 (and January 23, 2007) letter. As such we urge the Staff to not concur with the Company's conclusion that the Proposal is excludable as concerning the Company's ordinary business.

Conclusion

For the reasons given above and in our letters of January 23, 2007 and February 8, 2007 the Proponent, request that the Staff inform the Company that SEC proxy rules require denial of Verizon's no-action request. Please call me at (971) 222-3366 with any questions in connection with this matter, or if the Staff wishes any further information.

Thank you for your consideration of this matter.

Sincerely,



Jonas Kron
Attorney at Law

cc: Mary Louise Weber, Assistant General Counsel, Legal Department, Verizon
As You Sow Senior Staff
As You Sow Board of Directors
Thomas Van Dyck

DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the Company in support of its intention to exclude the proposals from the Company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes administered by the Commission, including argument as to whether or not activities proposed to be taken would be violative of the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversary procedure.

It is important to note that the staff's and Commission's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly a discretionary determination not to recommend or take Commission enforcement action, does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the management omit the proposal from the company's proxy material.

February 22, 2007

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: Verizon Communications Inc.
Incoming letter dated December 27, 2006

The proposal requests that the board issue a report on the technological, legal, and ethical policy issues surrounding the disclosure of customer records and communications content to government agencies without a warrant and non-governmental entities (e.g., private investigators), and their effect on customer privacy rights.

There appears to be some basis for your view that Verizon may exclude the proposal under rule 14a-8(i)(7), as relating to Verizon's ordinary business operations (i.e., procedures for protecting customer information). Accordingly, we will not recommend enforcement action to the Commission if Verizon 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 Verizon relies.

Sincerely,

Amanda McManus
Attorney-Adviser

END