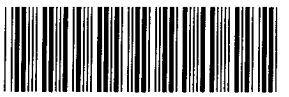
NO ACT

PE
2-17-09



09011564

DIVISION OF
CORPORATION FINANCE

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

February 27, 2009

Jonas Kron
Senior Social Research Analyst
Trillium Asset Management Corporation
711 Atlantic Avenue
Boston, MA 02111-2809

Act: 1934
Section:
Rule: 14a-8
Public
Availability: 2-27-09

Re: AT&T Inc.
Incoming letter dated February 17, 2009

Dear Mr. Kron:

This is in response to your letter dated February 17, 2009. In that letter, you requested that the Commission review the Division of Corporation Finance's January 26, 2009 no-action letter regarding the shareholder proposal submitted to AT&T by Trillium Asset Management Corporation on behalf of Jane Brown, Calvert Asset Management Company and Boston Common Asset Management. We have also received a letter from AT&T dated January 29, 2009.

Under Part 202.1(d) of Section 17 of the Code of Federal Regulations, the Division may present a request for Commission review of a Division no-action response relating to Rule 14a-8 under the Exchange Act if it concludes that the request involves "matters of substantial importance and where the issues are novel or highly complex." We have applied this standard to your request and determined not to present your request to the Commission.

Sincerely,

Thomas J. Kim
Chief Counsel & Associate Director

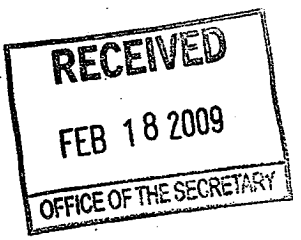
cc: David B. Harms
Sullivan & Cromwell LLP
125 Broad Street
New York, NY 10004-2498

TRILLIUM ASSET MANAGEMENT
25 Years of Investing for a Better World

Trillium Asset Management Corporation
www.trilliuminvest.com

Jonas Kron, J.D., M.S.E.L.
Senior Social Research Analyst
T: 971-222-3366
F: 617-482-6179
jkron@trilliuminvest.com

February 17, 2009



Ms. Elizabeth M. Murphy, Secretary
Securities & Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-9303

Re: Request for Commission review of no-action determination regarding shareholder proposal

Dear Ms. Murphy,

I write on behalf of Jane Brown, Trillium Asset Management Corporation, Calvert Asset Management Company, Inc. and Boston Common Asset Management (hereinafter referred to as "Proponents") in connection with a no-action determination issued by the Division of Corporation Finance (hereinafter referred to as the "Division") on January 26, 2009[1] in connection with a shareholder proposal (hereinafter referred to as the "Proposal") submitted by the Proponents to AT&T, Inc. (hereinafter referred to as "AT&T" or the "Company"). The Division letter is attached as Exhibit A.

Pursuant to 17 C.F.R. 202.1(d), the Proponents respectfully request that the Commission review the Division's determination and reverse the conclusion reached by the Division upholding the Company's view that it may exclude the Proposal from AT&T's proxy materials. The Proponents are long-term investors in the Company and own over 1,300,000 shares of AT&T common stock worth over $33 million.

As we explain more fully below, the Division's ruling qualifies for plenary review by the Commission under section 202.1(d) as it presents a novel issue of substantial importance to shareholders and registrants alike. Detailed legal arguments of the parties appear in AT&T's request for no-action relief, filed December 10, 2008 (Exhibit B) and the Proponents' opposition letter, dated January 9, 2009 (Exhibit C).

The Proposal

Report on Network Management Practices,
Public Expectations of Privacy and Freedom of Expression on the Internet

The Internet is becoming the defining infrastructure of our economy and society in the 21st century. Its potential to open markets for commerce, venues for cultural expression and modalities of civic engagement is without historic parallel.

Internet Service Providers (ISPs) are gatekeepers to this infrastructure: providing access, managing traffic, insuring communication, and forging rules that shape, enable and limit the public's Internet use.

As such, ISPs have a weighty responsibility in devising network management practices. ISPs must give far-ranging thought to how these practices serve to promote--or inhibit--the public's participation in the economy and in civil society.

Of fundamental concern is the effect ISPs' network management practices have on public expectations of privacy and freedom of expression on the Internet.

[1] The Proponents did not receive the no-action determination until Thursday February 5, 2009 – ten days after the date of the letter.

of ISPs have taken center stage in debates about free speech and public expectations of privacy. As more of our economic, social, political and cultural activities have moved online, ISPs are faced with new and profound questions about how to reconcile their roles as for-profit public companies with their responsibilities as content providers, news outlets, and protectors of public discourse and personal data. This issue was the subject of a November 30th analysis in the New York Times Magazine in which a leading expert, Professor Jeffery Rosen of George Washington University Law School, wrote:

> *As more and more speech migrates online, to blogs and social-networking sites and the like, the ultimate power to decide who has an opportunity to be heard, and what we may say, lies increasingly with Internet service providers, search engines and other Internet companies...*

The Proposal at issue originated with the controversial and widely publicized actions of AT&T in suppressing the voice of Eddie Vedder, lead singer of one of the most popular music groups in the world. On August 5, 2007, AT&T censored its webcast of a concert performance by the rock band Pearl Jam, blocking the audio feed when Eddie Vedder ad-libbed some non-obscene but politically pointed lyrics:

> "George Bush, leave this world alone."
> "George Bush find yourself another home."

AT&T did not voluntarily disclose the fact of the Company's censorship activities or their reasons for it until public attention and the resultant scrutiny and criticism became widely reported in the media.

Soon after the incident, Trillium engaged AT&T management in dialogue on this issue. The Company disclosed, subsequent to the Pearl Jam episode it had adopted a "new policy" regarding censorship, but that policy apparently applies only to similar web performances. In a series of correspondence between AT&T and Trillium (five letters in all), the Company would not disclose how freedom of speech is being treated in other service offerings where AT&T functions as a content provider.

Left without other options, Trillium exercised its rights as a shareholder to present the issue of free speech before fellow shareholders at the Company's 2009 annual meeting. As discussed in our letter to the Staff, a number of ISPs have been accused of engaging in censorship in very public ways – see, for example, Verizon's censorship of NARAL for "controversial material." For that reason, an identical proposal was filed by the Proponents and other shareholders at Charter Communications, Embarq, Verizon, CenturyTel, Sprint Nextel, Knology, Comcast and Qwest.

Shareholders are legitimately concerned about the strategic implications of these developments on the Company and society. We believe AT&T has not comprehensively addressed the issues and is, at best, utilizing an ad hoc method of protecting freedom of speech and privacy issues. AT&T's management seeks to deny shareholders the opportunity to consider these issues at the Company's annual meeting by arguing that the Proposal focuses on mundane matters. As demonstrated below, the Proposal focuses on issues that present significant strategic challenges to the Company and implicate some of our most valuable civil liberties.

The Division's Determination

AT&T argued the Proposal may be excluded from the Company's 2009 proxy statement by virtue of Rules 14a-8(i)(7) and 14a-8(i)(10). Specifically, the Company maintained that the Proposal should be excluded under Rule 14a-8(i)(7) for relating to "procedures for protecting customer information"; for focusing on a legal compliance program; and for directing company lobbying efforts. Under Rule 14a-8(i)(10) the Company argued that its privacy policies and public statements demonstrated that it had substantially implemented the Proposal.

This significant body of evidence of a widespread public debate, on the issues of public expectations of privacy and freedom of expression, goes far beyond the requirements of the Rule. Most importantly, the Company does nothing in either letter to argue that these issues are somehow less important than we demonstrate. *The Company has done nothing to demonstrate that public expectations of privacy and freedom of speech are not significant policy issues confronting the Company.* For that reason alone, it has failed to meet its burden of proof on this point.

The fact that privacy issues are significant policy issues is perhaps best shown through the Company's own assertion they are a significant policy issue. On August 13, 2008 AT&T's Senior Vice-President – Public Policy and Chief Privacy Officer, Dorothy Attwood, wrote a letter to Congress in response to inquiries about the use of deep packet inspection (an Internet filtering technology that enables data mining, eavesdropping, and censorship). In that letter, Ms. Attwood stated that Congress was right to be concerned because these capabilities posed "***significant policy questions.***"

The following month, on September 25, 2008, in Ms. Attwood's testimony to Congress on the same issue, she stated "***Your interest in these matters surely is warranted.***" (emphasis added). She went on to state these kinds of technologies "that involve tracking consumer web browsing and search activities, ***raise important consumer-privacy concerns that policymakers and industry must carefully weigh.***" (emphasis added).

As further significant public policy evidence, we strongly urge the Commission to consider the very recent conclusions of its sister agency, the Federal Trade Commission ("FTC"). On February 12, 2009 the FTC issued a report entitled "Self-Regulatory Principles For Online Behavioral Advertising " which focuses on privacy concerns. Specifically, the Report observes "the ease with which companies can collect and combine information from consumers online has raised questions and concerns about consumer privacy." The Report further expresses concerns about the numerous threats to the privacy of Internet users. See attached copy of Report (Exhibit D).

The Report discussed a number of recent developments in the area of privacy, many of which we raised in our January 9, 2009 letter, including:

- the emergence of new online privacy tools;
- a Network Advertising Initiative publication of new privacy principles;
- the announcement of a joint industry task force including marketing and industry trade associations, as well as the Council of Better Business Bureaus, of a cooperative effort to develop self-regulatory principles to address privacy concerns related to online behavioral advertising ;
- the privacy initiatives of the Future of Privacy Forum, Center for Democracy and Technology, and TRUSTe;
- the July 9, 2008 and September 25, 2008 Senate Committee on Commerce, Science, and Transportation hearings entitled "Privacy Implications of Online Advertising," at which a n AT&T representative testified;
- the July 17, 2008, House Telecommunications Subcommittee hearing entitled "What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies" ; and
- on August 1, 2008, four members of the House Committee issued letters to thirty-four companies seeking information on their practices with respect to behavioral advertising.

After that discussion, the Report concluded:

> These developments suggest that there is ***continuing public interest in the issues*** that behavioral advertising raises and increasing engagement by industry members in developing solutions.

Report at page 17 (emphasis added). It has been observed this is the Internet industry's last chance to get privacy issues right and the FTC concluded:

- Privacy policies are not a good enough way to tell people what information is being collected about them.
- The privacy of users is not necessarily protected because a system doesn't capture names or other "personally identifiable information."
- The industry's self regulation has not been adequate; and
- Internet companies have not cooperated with the commission to provide enough information on what is happening now with data about users.

January 26, 2009

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: AT&T Inc.
Incoming letter dated December 10, 2008

The proposal requests the board to issue a report examining the effects of AT&T's internet network management practices.

There appears to be some basis for your view that AT&T may exclude the proposal under rule 14a-8(i)(7), as relating to AT&T's ordinary business operations (i.e., procedures for protecting user information). Accordingly, we will not recommend enforcement action to the Commission if AT&T omits the proposal from its proxy materials in reliance on rule 14a-8(i)(7). In reaching this position, we have not found it necessary to address the alternative basis for omission upon which AT&T relies.

Sincerely,

Philip Rothenberg
Attorney-Adviser

SULLIVAN & CROMWELL LLP

TELEPHONE: 1-212-558-4000
FACSIMILE: 1-212-558-3588
WWW.SULLCROM.COM

125 Broad Street
New York, NY 10004-2498

LOS ANGELES • PALO ALTO • WASHINGTON, D.C.
FRANKFURT • LONDON • PARIS
BEIJING • HONG KONG • TOKYO
MELBOURNE • SYDNEY

December 10, 2008

Via Federal Express

Mr. Jonas Kron,
Senior Social Research Analyst,
Trillium Asset Management Corp.,
711 Atlantic Avenue,
Boston, MA 02111-2809.

Dear Sir:

On behalf of my client, AT&T, Inc. (the "Company"), enclosed is a copy of a letter, including annexes, filed with the SEC in connection with the stockholder proposal you submitted to the Company in a letter dated October 28, 2008 on behalf of Jane Brown.

Sincerely,

Alexander Rakosi
Sullivan & Cromwell LLP

(Enclosure)

SULLIVAN & CROMWELL LLP

TELEPHONE: 1-212-558-4000
FACSIMILE: 1-212-558-3588
WWW.SULLCROM.COM

125 Broad Street
New York, NY 10004-2498

LOS ANGELES • PALO ALTO • WASHINGTON, D.C.
FRANKFURT • LONDON • PARIS
BEIJING • HONG KONG • TOKYO
MELBOURNE • SYDNEY

December 10, 2008

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

Re: AT&T Inc. – Request to Exclude Stockholder Proposal of Trillium Asset Management Corp. on behalf of Jane Brown and Co-Proponents

Ladies and Gentlemen:

Our client, AT&T Inc., a Delaware corporation ("AT&T" or the "Company"), proposes to exclude a stockholder proposal this year for the same reason the Commission staff (the "Staff") permitted the Company to exclude substantially the same proposals the last two years, as well as the other reasons described in this letter.[1] We believe the current proposal is merely an attempt to repackage the proposals from the last two years about AT&T's management function regarding its customer privacy practices, each of which the Staff concluded was excludable on ordinary business grounds under item (i)(7) of Rule 14a-8. We also believe the current proposal is excludable under item (i)(10) on the ground that it has already been substantially implemented.

On behalf of AT&T, we respectfully request the Staff to confirm that it will not recommend any enforcement action to the Commission if the Company excludes this year's stockholder proposal (the "Current Proposal") by Trillium Asset Management Corp. on behalf of Jane Brown (the "Proponent") from its proxy statement and proxy card for the 2009 annual meeting.

[1] Certain of the factual information in this letter was provided to us by the Company.

Boston Common Asset Management, LLC ("Boston Common"), on behalf of certain of its clients, and Calvert Asset Management Company, Inc. ("Calvert"), on behalf of certain of its related funds, have also submitted proposals to the Company that are identical to the Current Proposal and have asked to join the Proponent as co-filers of the Current Proposal. Thus, our request to confirm that the Current Proposal may be excluded from the Company's 2009 proxy statement applies with regard to these co-filers' submissions as well.

The Company currently plans to file its definitive proxy statement for the 2009 annual meeting on or about March 11, 2009, which is more than 80 days after the date of this letter. Pursuant to Rule 14a-8(j), we enclose six paper copies of this letter, together with the Current Proposal, the Proponent's cover letter and supporting statement and the co-filer's submissions. We have also sent copies of this letter and the accompanying documents to the Proponent, to the attention of its designated contact, Jonas Kron of Trillium Asset Management Corp., to Boston Common, to the attention of its designated contact, Melissa Locke, and to Calvert, to the attention of its designated contact, Aditi Vora.

The Current Proposal

The Current Proposal is entitled "Report on Network Management Practices, Public Expectations of Privacy and Freedom of Expression on the Internet". Following several paragraphs of introductory language, the Current Proposal sets forth the following resolution to be adopted by stockholders at the 2009 annual meeting:

> "Therefore, be it resolved, that stockholders request the board to issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet."

The full text of the Current Proposal and the Proponent's supporting statement, as well as related correspondence with the Proponent, Boston Common and Calvert, are attached as Annex A.

The Prior Proposals

The Current Proposal is substantially the same as stockholder proposals submitted to the Company in each of the last two years for consideration at its 2007 and 2008 annual meetings (the "Prior Proposals") and which the Staff permitted the Company to exclude from its 2007 and 2008 proxy statements pursuant to item (i)(7) of Rule 14a-8. See Letters regarding *AT&T Inc.* (February 9, 2007 and February 7, 2008). Like the Current Proposal, the Prior Proposals were also co-filed by Calvert. The Prior Proposals, had they been adopted, would have requested the Company's Board of Directors (the "Board") to prepare a report that discussed, in the words of last year's version, "the policy issues that pertain to disclosing customer records and the content of customer

communications to federal and state agencies without a warrant, as well as the effect of such disclosure on the privacy rights of customers".[2] The Staff concluded that AT&T could exclude the Prior Proposals because they related, in the case of last year's version, "to AT&T's ordinary business operations (i.e., procedures for protecting customer information)."[3]

As described in more detail below, the Current Proposal addresses a topic that, at its core, is the same as the topic addressed by the Prior Proposals, namely, AT&T's management practices relating to customer privacy. Whereas the Prior Proposals requested the Board to prepare a report on customer privacy practices including, among other things, disclosure of information to government agencies, the Current Proposal requests a Board report on customer privacy practices as they relate to the Internet. While the wording of the Prior Proposals made reference to government agencies and the wording of the Current Proposal makes reference to the Internet, all three proposals are phrased broadly enough to encompass a wide and overlapping range of customer privacy practices generally. Like the excluded Prior Proposals, the Current Proposal is equally focused on management functions regarding customer privacy – that is, on the Company's ordinary business operations.

As discussed below, the Current Proposal is an attempt by stockholders to influence an aspect of the Company's ordinary business operations – customer privacy practices – that is the responsibility of management. These functions involve a host of complex technical, legal and financial issues that cannot be overseen or directed effectively by stockholders and for this reason have traditionally and properly been regarded as being within the province of management. In addition, the Company has already published a comprehensive statement of its privacy policies, procedures and practices, including those relating to the Internet, so that the core elements of the Current Proposal have already been substantially implemented.

Background Note

By way of background, the Company believes it is clear that the Prior Proposals as well as the Current Proposal were prompted by allegations, initially made in December 2005, that the Company disclosed certain private customer information to the National Security Agency (the "NSA") and other government agencies. Over 20 lawsuits based

---

[2] The earlier version, submitted in 2006, made substantially the same request: that the Board prepare a report on, among other things, "the overarching technical, legal and ethical policy issues surrounding (a) disclosure of the content of customer communications and records to the Federal Bureau of Investigation, NSA and other government agencies without a warrant and its effect on the privacy rights of AT&T's customers and (b) notifying customers whose information has been shared with such agencies". Given the substantial similarity of the Prior Proposals, for convenience our discussion of them focuses on last year's version except where noted.

[3] In the case of the earlier version, the Staff concluded it could be excluded because it related to "AT&T's ordinary business operations (i.e., litigation strategy)." The litigation referenced by the Staff involves the allegations that AT&T disclosed customer information to government agencies and is discussed further below.

on those allegations were filed against the Company in federal district courts throughout the United States, the first one in January 2006. See *Hepting v. AT&T,* No. 3:06-CV-006720-VRW (N.D. Cal.). The lawsuits making the same allegations were subsequently consolidated in the U.S. District Court for the Northern District of California. The district court denied motions to dismiss the case made by both the U.S. Government and the Company, which then appealed the decision to the U.S. Court of Appeals for the Ninth Circuit. While the appeal was pending, Congress and the President enacted legislation intended to grant immunity to telecommunications companies, such as AT&T, with respect to lawsuits based on their alleged cooperation with government agencies, in each case if the U.S. Attorney General requested that the relevant lawsuit be dismissed. The Ninth Circuit remanded the case against the Company to the district court for reconsideration in light of the new statute, and the Attorney General subsequently requested that the case be dismissed. The plaintiffs then challenged the statute on constitutional grounds, and that challenge is now pending before the district court.

Both of the Prior Proposals made specific reference to the allegations in the lawsuit and asked the Board to report on the Company's privacy practices in light of those allegations. The Company requested and the Staff granted no-action relief allowing the Company to exclude those proposals from the Company's annual proxy statements for 2007 and 2008, respectively. While the Current Proposal does not refer specifically to these allegations, the Company believes that the Current Proposal, as much as each of the Prior Proposals, reflects an attempt to address matters that are the subject of the pending judicial proceeding as well as the earlier legislative proceeding in Congress. These matters are being addressed through the judicial and legislative processes and the Company believes it is not appropriate to address them, directly or indirectly, through the proxy solicitation process.

In addition, the Current Proposal would require the Board, in very broad terms, to report on the Company's Internet network management practices in the context of "the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet." Given the sweeping scope of this request, as well as the judicial and legislative proceedings that provide the backdrop to this request, it would be difficult for the requested report to avoid discussion of the allegations made in pending lawsuits – including the litigation alleging that AT&T has in the past disclosed private customer information to the NSA and other government agencies and that any such disclosure violated the privacy rights of AT&T customers – or, therefore, to avoid discussion about whether those allegations are true or false. The Company believes, however, that any such discussion would be difficult to have in any meaningful way without providing potentially sensitive information relating to the events in question, information that, if made public, could raise questions about whether such disclosure was lawful. While the Current Proposal purports to allow the Board to exclude "proprietary and confidential information", it pertains to matters that are inherently sensitive and may even be subject to federal statutory or other legal restrictions on disclosure relating to national security and law enforcement. In its letters to the Staff regarding the Prior Proposals, the Company provided a detailed explanation of why such requested reports could cause AT&T to violate federal laws designed to

protect the intelligence gathering activities of the U.S. Government. Given the sweeping breadth of the Current Proposal, those concerns remain relevant this year, and we refer the Staff to the Company's discussion of those concerns in its prior letters.

The Current Proposal Relates to Ordinary Business Matters and May Be Excluded Pursuant to Rule 14a-8(i)(7)

Item (i)(7) of Rule 14a-8 permits a company to omit a stockholder proposal from its proxy materials if the proposal deals with a matter relating to the company's ordinary business operations. The general policy underlying the "ordinary business" exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual stockholders meeting." This general policy reflects two central considerations: (1) "certain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight" and (2) the "degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Exchange Act Release No. 34-40018 (May 21, 1998).

In applying the item (i)(7) exclusion to proposals requesting companies to prepare reports on specific aspects of their business, the Staff has determined that it will consider whether the subject matter of the report involves a matter of ordinary business. If it does, the proposal can be excluded even if it requests only the preparation of the report and not the taking of any action with respect to such ordinary business matter. Exchange Act Release No. 34-20091 (August 16, 1983).[4]

The Current Proposal Relates to Matters of Customer Privacy

The Current Proposal can be omitted under item (i)(7) because it seeks to subject to stockholder oversight AT&T's policies and procedures for protecting customer privacy[5] in the context of its Internet network management practices. The development and implementation of these policies and procedures are an integral part of AT&T's day-to-day business operations and a function that is properly and necessarily left to the discretion of management.

Customer Privacy Is a Management Function. The Staff has long recognized that the protection of customer privacy is a core management function, not subject to stockholder oversight, and has, to that end, allowed companies to exclude proposals requesting reports on issues related to customer privacy. In *Verizon Communications*

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

[5] The Current Proposal also refers to customer freedom of expression, a topic that is closely related to and largely overlaps with customer privacy and is addressed further below.

Inc., a stockholder submitted a proposal requesting that the company prepare a report describing "the overarching technological, legal and ethical policy issues surrounding the disclosure of customer records and communications content" to government and non-government agencies. The proposal also emphasized the importance of these issues in terms of customer freedom of expression. Notwithstanding these concerns, the Staff allowed Verizon to exclude the proposal from its proxy materials on the ground that it related "to Verizon's ordinary business operations (*i.e.*, procedures for protecting customer information)." See Letter regarding *Verizon Communications Inc.* (February 22, 2007). In essence, the subject matter of the Current Proposal is substantially the same as that addressed in *Verizon Communications Inc.*, because its underlying premise relates to the way the Company protects and handles the privacy of customer information, in this instance in the context of Internet network management practices.

Similarly, in *Bank of America Corp.*, a stockholder, in response to specific instances of lost and stolen customer records, submitted a proposal requesting that the company prepare a report on its policies and procedures for ensuring the confidentiality of customer information. The Staff concluded that the requested report involved matters of ordinary business in that it sought information regarding the company's "procedures for protecting customer information" and concurred in the company's decision to exclude the proposal pursuant to Rule 14a-8(i)(7). See Letter regarding *Bank of America Corp.* (February 21, 2006); see also Letters regarding *Bank of America Corp.* (March 7, 2005) (almost identical proposal from the same proponent could be excluded as relating to the company's ordinary business of protecting customer information); *Applied Digital Solutions, Inc.* (March 25, 2006) (proposal requesting the company to prepare a report analyzing the privacy implications of its radio frequency identification chips could be excluded as relating to the company's ordinary business of managing privacy issues related to product development); *Citicorp* (January 8, 1997) (proposal requesting the company to prepare a report on policies and procedures to monitor illegal transfers through customer accounts could be excluded as relating to ordinary business operations).

Equally relevant are the Staff's earlier decisions to permit AT&T to exclude the Prior Proposals from the 2007 and 2008 proxy statements. The Staff concluded that the Prior Proposals, which were substantially identical to the proposals considered in Verizon Communications Inc. and Bank of America Corp., related to AT&T's ordinary business operations, in particular to aspects of the Company's procedures for protecting customer information. The very same procedures, this time in the context of Internet network management practices, are now the focus of the Current Proposal.

While phrased somewhat more broadly than the Prior Proposals and the proposals in *Verizon Communications Inc.* and *Bank of America Corp.*, the Current Proposal focuses on precisely the same ordinary business operations at issue in those other no-action letters. The Current Proposal would require AT&T to produce a report examining "the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet." Such a report would inevitably require the

Company to address the way it handles customer information with regard to privacy concerns – in other words, to address its policies and procedures relating to customer privacy in the context of Internet usage. As noted above, the Staff has long recognized that matters of customer privacy in general are necessarily part of ordinary business operations.

Thus, just like the Prior Proposals and those in *Verizon Communications Inc.* and *Bank of America Corp.*, the Current Proposal focuses directly on the Company's policies and procedures for protecting customer information, in this case in the context of Internet usage, and in particular on certain commercial aspects of this topic. As the Staff has already recognized, matters of this kind are integral to the day-to-day business operations of a company and cannot, "as a practical matter, be subject to direct shareholder oversight." Exchange Act Release No. 34-40018 (May 21, 1998).

Public Policy Overlap Does Not Change the Outcome. Additionally, it should be noted that the fact that a proposal touches upon a matter with possible public policy implications does not necessarily undermine the basis for omitting it under item (i)(7). The Staff has indicated that the applicability of item (i)(7) depends largely on whether implementing a proposal would have broad public policy impacts outside the company, or instead would deal with matters of the company's internal business operations, planning and strategies. In fact, the Staff has consistently concurred with the exclusion of proposals that address ordinary business matters, even though they might also implicate public policy concerns. See, *e.g.*, Letters regarding *Microsoft Corporation* (September 29, 2006) (excluding proposal asking the company to evaluate the impact of expanded government regulation of the Internet); and *Pfizer Inc.* (January 24, 2006) and *Marathon Oil* (January 23, 2006) (in both cases, excluding proposals requesting inward-looking reports on the economic effects of HIV/AIDS, tuberculosis and malaria pandemics on the company's business strategies and risk profiles). As noted above, the Current Proposal is directed at Internet network management practices, privacy policies and procedures and a number of related business, financial, technical and legal issues and thus falls squarely in this group.

The Current Proposal Relates to Matters of Legal Compliance

The Current Proposal can also be properly excluded pursuant to item (i)(7) because it relates to the Company's conduct of its legal compliance program. The Staff has long identified a company's compliance with laws and regulations as a matter of ordinary business. In *Allstate Corp.*, a stockholder proposal requested, in part, that the company issue a report discussing the illegal activities that were the subject of a number of state investigations and consent decrees involving Allstate. The Staff held that a company's general conduct of a legal compliance program was a matter of ordinary business and agreed to Allstate's exclusion of the proposal under Rule 14a-8(i)(7). Letter regarding *Allstate Corp.* (February 16, 1999); see also Letters regarding *Duke Power Co.* (February 1, 1988) (proposal requesting the company to prepare a report detailing its environmental protection and pollution control activities could be excluded as relating to

the ordinary business of complying with government regulations); and *Halliburton Company* (March 10, 2006) (proposal requesting a report addressing the potential impact of certain violations and investigations on the company's reputation and stock value and how the company intended to prevent further violations could be excluded as relating to the ordinary business of conducting a legal compliance program).

Legal compliance is exactly the type of "matter of a complex nature upon which stockholders, as a group, would not be in a position to make an informed judgment" (Exchange Act Release No. 34-40018 (May 21, 1998)). Moreover, stockholder interference with legal compliance poses a significant risk of micro-managing the company.

As already noted, the Current Proposal requests a report about the Company's Internet network management practices insofar as they affect customer privacy interests. A report on this topic would inevitably lead to a discussion of the Company's compliance with laws and regulations governing the use of customer information and customer privacy. In addition, as also noted above, the Proponent's supporting statement makes it clear that the report would need to address the Company's practices regarding disclosure of customer information to third parties, which in turn would likely require a discussion of disclosure to government agencies on law enforcement or national security grounds. This part of the Current Proposal may well lead to a re-examination of the allegations that are the basis of the pending lawsuit against the Company and that were a particular focus of the Prior Proposals. As noted above, the Company believes that this aspect of the Current Proposal could raise some of the concerns about the potential violation of federal disclosure laws that were discussed in the Company's letters to the Staff regarding the Prior Proposals.

The legal and compliance issues relating to customer privacy are complex and rapidly evolving. This is particularly true with regard to laws and regulations governing the use of the Internet, as this is an area of the law that is closely intertwined with the many technological developments affecting the Internet. It is also particularly true with regard to laws and regulations relating to disclosure to government agencies, as these raise difficult questions about law enforcement and national security. In sum, the Current Proposal would require the Company to address with its stockholders precisely the kind of complex legal and compliance issues about which stockholders are not in a position to make an informed judgment and that the Staff has long recognized comprise ordinary business operations and are properly the responsibility of management.

The Current Proposal Involves the Company in the Political or Legislative Process

The Current Proposal may also be excluded under item (i)(7) because it would involve the Company in the political or legislative process relating to aspects of the Company's operations. A number of no-action letters have confirmed that proposals requesting a company to issue reports analyzing the potential impact on the company of proposed

national legislation may properly be excluded as "involving [the company] in the political or legislative process relating to an aspect of [the company's] operations." See Letters regarding *International Business Machines Corp.* (March 2, 2000), *Electronic Data Systems Corp.* (March 24, 2000) and *Niagara Mohawk Holdings, Inc.* (March 5, 2001) (in all three cases, proposals requesting the company to issue reports evaluating the impact on the company of pension-related proposals being considered by national policy makers were excluded on the ground that they could involve the company in the political or legislative process).

Preparing a report for stockholders about Internet network management practices in the context of customer privacy and freedom of expression, as the Current Proposal calls for, would require the Company to address publicly a number of difficult technical, legal and business issues that are currently the subject of sometimes intense and controversial debate among federal and state legislators, regulators, the media and the public. For example, one of the most intensely debated issues relating to Internet network management practices in recent years involves the concept of "net neutrality" – *i.e.*, whether Internet service providers should be required to implement non-discrimination safeguards designed to prevent them from blocking, speeding up or slowing down web content based on its source, ownership or destination. A bill to amend the Communications Act of 1934 to establish certain Internet neutrality duties for Internet service providers was read twice in Congress[6] and has been referred to the U.S. Senate Committee on Commerce, Science and Transportation, but has not yet been passed. Therefore, this topic remains subject to legislative and political debate and has not been resolved. The same may be said for the disclosure of Internet customer information to government agencies on law enforcement or national security grounds.

Requiring the Company to address these matters in a detailed, public way, including by examining the many social, political and other "significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet", as the Current Proposal states, would force the Company to involve itself in an ongoing political and legislative debate that could have far reaching effects on its business and operations. Topics such as net neutrality and disclosure to government agencies require a careful evaluation of complex, fact-specific issues that implicate a number of business, financial, technological and legal considerations. It is neither appropriate nor effective to conduct this kind of an evaluation through the proxy solicitation process and doing so could harm interests of the Company and its stockholders.

The Staff has recognized that stockholder proposals need not be included in proxy statements if they would force a company to engage in a political or legislative debate that could affect its ordinary business operations. In fact, the Staff recently re-affirmed this position with regard to stockholder proposals requiring reports about Internet network management practices and net neutrality. See Letters regarding *Yahoo, Inc.*

---

[6] See the 110th session of the Congress; S. 215, 110th Cong. (2007).

(April 5, 2007) and *Microsoft Corporation* (September 29, 2006) (requests for reports evaluating the impact of expanded government regulation of the Internet, particularly with regard to net neutrality, could be excluded under item (i)(7)). In light of the foregoing, the Current Proposal should be excludable under item (i)(7) as one that would involve the Company in the political or legislative process affecting its ordinary business operations.

The Current Proposal Has Been Substantially Implemented and May be Omitted Pursuant to Rule 14a-8(i)(10)

The Company's Privacy Policy Itself Represents Substantial Implementation

AT&T believes that the Current Proposal may also be omitted from the 2009 proxy materials because it has already published its Privacy Policy, which is the official statement of the Company's policies and procedures regarding customer privacy. These policies and procedures would be the core of any report that the Board would issue if the Current Proposal were adopted. The Privacy Policy is posted on the Company's website and is readily available to all stockholders, thus providing them with the basic information they need to evaluate the Company's policies and procedures concerning customer privacy, including in the context of the Company's Internet network management practices. Consequently, the Company believes that the Current Proposal has been substantially implemented and may be excluded from the 2009 proxy materials under item (i)(10) of Rule 14a-8.

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

The Staff has also established that a company does not have to implement every detail of a proposal in order to exclude it under item (i)(10). Rather, "substantial implementation" requires only that the company's actions "satisfactorily address the underlying concerns of the proposal." Letter regarding *Masco Corp.* (March 29, 1999); see also, Letter regarding *Entergy, Inc.* (January 31, 2006).

The underlying concern of the Current Proposal relates to the safeguards the Company has put in place to ensure protection of the public's expectations of privacy and freedom of expression on the Internet and the way the Company is handling information with respect to its customers. AT&T's Privacy Policy[7], which is available on the Company's website at http://att.com, already covers the Company's current policies, practices and procedures for protecting the confidentiality of customer information, including what customer information is collected and how it can be used, when and to whom it may be disclosed (including to law enforcement and other government agencies) and how the Company implements and updates its privacy policies, practices and procedures. In particular, the item titled "What Online Information We Collect, How We Use It and How You Can Control Its Use" explains, among other things, web usage information, email marketing practices and online privacy education. With respect to the latter point, AT&T's strong commitment to protect privacy rights and its efforts to constantly enhance security in connection with Internet use are also evidenced by the fact that the Privacy Policy contains detailed information on how to better protect customers' privacy and security while online. For that purpose, the Company provides its Internet customers with tools such as the "AT&T Internet Safety Web site" and the "AT&T Worldnet Security Center", which allow these customers to acquire the most recent available information and the best technical support in order to be optimally protected when using the Company's internet services.

Furthermore, the Privacy Policy provides that personal identifying information may be provided to third parties only when permitted or required by law and only in a limited number of specific instances, for example "to notify a responsible governmental entity if we reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without delay."

The Privacy Policy squarely addresses the underlying concern of the Current Proposal, namely, the policies, procedures and practices AT&T follows in order to protect the privacy of its customers with regard to their use of the Internet. These policies, procedures and practices, as reflected in the Privacy Policy, would necessarily form the core of any report the Board would issue if the Current Proposal were adopted. Consequently, the Privacy Policy already provides stockholders with the essential information they need to understand and evaluate how the Company addresses customer privacy matters in the context of its Internet network management practices. Requiring the Board to prepare a report on this topic would add little of real substance to the information that is already available to stockholders on this topic.

[7] A copy of AT&T's Privacy Policy is also attached to this letter as Annex B.

The Company's Public Statements Have Further Implemented the Current Proposal

The Company has also provided the information called for by the Current Proposal in various public statements, as recently evidenced by the statement of Dorothy Attwood (Senior Vice President, Public Policy & Chief Private Officer) before the U.S. Senate Committee on Commerce, Science and Transportation at the Hearing on Broadband Providers and Consumer Privacy on online behavioral advertising on September 25, 2008.[8] Underscoring the Company's commitment to privacy protection, Ms. Attwood noted that "[W]e do, however, believe it is essential to include strong privacy protections in the design of any online behavioral advertising program, which is why we will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to ensure the protection of, and ultimate consumer control over, consumer information. We further intend to work with privacy advocates, consumer privacy coalitions and fellow industry participants in a cooperative, multi-faceted effort that we trust can and will lead to a predictable consumer driven framework in this area. In any event, if AT&T deploys these technologies and processes, it will do so the right way."

Similarly, the Company has made it clear in the public record that it is a vigorous proponent of freedom of expression on the Internet, most recently in the testimony of Robert W. Quinn, Jr. (Senior Vice President-Federal Regulatory) before the Federal Communications Commission on July 21, 2008 during a hearing on Broadband and the Digital Future: ".... and we respect free expression as a cornerstone of our free society. As a matter of long-standing policy, AT&T has not and will not suspend, disconnect or terminate service because of the views our customers express on any subject, including on public policy, political or social issues, or even if you just want to complain about something that we, AT&T, have or have not done. However, AT&T clearly advises customers that the use of our services for illegal purposes (such as the distribution of child pornography), or to threaten or endanger the health or safety of others, is strictly prohibited."[9]

Based on the considerations discussed above, AT&T believes that the Current Proposal may be omitted from its proxy materials pursuant to Rule 14a-8(i)(10) because it has already developed, implemented and made publicly available a comprehensive Privacy Policy and supplemented the Privacy Policy with numerous official, publicly available statements about important policy considerations relating to customer privacy and freedom of expression in the context of the Internet. These actions taken by the Company "compare favorably with the guidelines of the proposal" and substantially address the matters that lie at the heart of the Current Proposal.

---

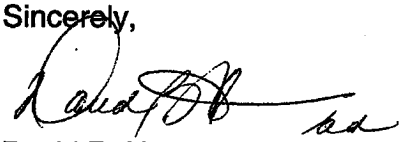
[8] The complete statement can be found under http://commerce.senate.gov/public/_files/AttwoodTestimony.pdf and is also attached as Annex C.

[9] The complete statement can be found under http://attpublicpolicy.centralcast.net/2008/07/fcc-testimony.php.

* * * * * * * * *

For the reasons set forth in this letter, we respectfully request the Staff to confirm that the Company may omit the Current Proposal from its 2009 proxy statement and proxy card in reliance on either or both of items (i)(7) and (i)(10) of Rule 14a-8. If you would like to discuss this request, please feel free to contact the undersigned by telephone at (212) 558-3882 or e-mail at harmsd@sullcrom.com.

Sincerely,



David B. Harms
Sullivan & Cromwell LLP

Enclosures

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

Jonas Kron
Senior Social Research Analyst
Trillium Asset Management Corp.

Melissa Locke
Social Research & Advocacy Analyst
Boston Common Asset Management, LLC

Aditi Vora
Social Research Analyst
Calvert Asset Management Company, Inc.

ANNEX A

Proposal/Co-proposals and related materials

TRILLIUM ASSET MANAGEMENT
25 Years of Investing for a Better World

Trillium Asset Management Corporation
www.trilliuminvest.com

October 28, 2008

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

Dear Ms. Meuleman,

Trillium Asset Management Corp. ("Trillium") is an investment firm based in Boston specializing in socially responsible asset management. We currently manage about $1 billion for institutional and individual clients.

I am hereby authorized to notify you of our intention to file the enclosed shareholder resolution with AT&T on behalf of our client, Ms. Jane Brown. Trillium submits this shareholder proposal for inclusion in the 2009 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, Ms. Brown holds more than $2,000 of AT&T common stock, acquired more than one year prior to this date. Ms. Brown will remain invested in this position through the date of the 2009 annual meeting. Verification of ownership from our custodian is attached. We will send a representative to the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

Please direct any communications to myself at (971) 222-3366, or via email at jkron@trilliuminvest.com

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

Sincerely,

Jonas Kron
Senior Social Research Analyst

BOSTON
711 Atlantic Avenue
Boston, Massachusetts 02111-2809
T: 617-423-6655 F: 617-482-6179
800-548-5684

DURHAM
353 West Main Street, Second Floor
Durham, North Carolina 27701-3215
T: 919-688-1265 F: 919-688-1451
800-853-1311

SAN FRANCISCO
369 Pine Street, Suite 711
San Francisco, California 94104-3310
T: 415-392-4806 F: 415-392-4535
800-933-4806

BOISE
950 W. Bannock Street, Suite 530
Boise, Idaho 83702-6118
T: 208-387-0777 F: 208-387-0278
800-567-0538

Report on Network Management Practices,
Public Expectations of Privacy and Freedom of Expression on the Internet

The Internet is becoming the defining infrastructure of our economy and society in the 21st century. Its potential to open markets for commerce, venues for cultural expression and modalities of civic engagement is without historic parallel.

Internet Service Providers (ISPs) are gatekeepers to this infrastructure: providing access, managing traffic, insuring communication, and forging rules that shape, enable and limit the public's Internet use.

As such, ISPs have a weighty responsibility in devising network management practices. ISPs must give far-ranging thought to how these practices serve to promote--or inhibit--the public's participation in the economy and in civil society.

Of fundamental concern is the effect ISPs' network management practices have on public expectations of privacy and freedom of expression on the Internet.

Whereas:

- More than 211 million Americans--70% of the population--use the Internet;
- The Internet serves as an engine of opportunity for social, cultural and civic participation in society;
- 46% of Americans have used the internet, e-mail or text messaging to participate in the 2008 political process;
- The Internet yields significant economic benefits to society, with online U.S. retailing revenues – only one gauge of e-commerce - exceeding $200 billion in 2008;
- The Internet plays a critical role in addressing societal challenges such as provision of health care, with over 8 million Americans looking for health information online daily;
- 72% of Americans are concerned that their online behaviors are being tracked and profiled by companies;
- 54% of Americans are uncomfortable with third parties collecting information about their online behavior;
- Our Company provides Internet access to a very large number of subscribers and is considered a leading ISP;
- Our Company's network management practices have been questioned by consumers, civil liberties groups and shareholders; specifically, AT&T was scrutinized for censoring political speech; was the focus of a BusinessWeek story discussing content monitoring; and was called before Congress to testify on these issues;

- Class action lawsuits in several states are challenging the propriety of ISPs' network management practices;

- Internet network management is a significant public policy issue; failure to fully and publicly address this issue poses potential competitive, legal and reputational harm to our Company;

- Any perceived compromise by ISPs of public expectations of privacy and freedom of expression on the Internet could have a chilling effect on the use of the Internet and detrimental effects on society.

Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet.

Supporting Statement

One example of an issue to be examined could be the social and political effects of collecting and selling personal information to third-parties, including information companies such as First Advantage and Equifax.

Shelley Alpern
Director of Social Research & Advocacy
Trillium Asset Management Corp.
711 Atlantic Avenue
Boston, MA 02111

Fax: 617 482 6179

Dear Ms. Alpern:

I hereby authorize Trillium Asset Management Corporation to file a shareholder resolution on my behalf at AT&T Inc. (T).

I am the beneficial owner of 200 shares of AT&T Inc. (T) common stock that I have held for more than one year. I intend to hold the aforementioned shares of stock through the date of the company's annual meeting in 2009.

I specifically give Trillium Asset Management Corporation full authority to deal, on my behalf, with any and all aspects of the aforementioned shareholder resolution. I understand that my name may appear on the corporation's proxy statement as the filer of the aforementioned resolution.

Sincerely,

Jane Brown
c/o Trillium Asset Management Corporation
711 Atlantic Avenue, Boston, MA 02111

10/27/08
Date

charles SCHWAB
INSTITUTIONAL

PO Box 628290 Orlando Florida 32862-8290

October 28, 2008

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

Re: Jane Brown/Schwab Account*** FISMA & OMB Memorandum M-07-16 ***

Dear Ms. Meuleman :

This letter is to confirm that Charles Schwab & Company holds as custodian for the above account more than $2,000 (two thousand dollars) worth of common stock in AT&T Inc. (T). These shares have been held continuously for at least on year prior to and through October 28, 2008.

The shares are held at Depository Trust Company under the Nominee name of Charles Schwab and Company, Inc.

This letter serves as confirmation that the account holder listed above is the beneficial owner of the above referenced stock.

Sincerely,

Jake Carris

BOSTON COMMON
ASSET MANAGEMENT, LLC

November 10, 2008

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

Dear Ms. Meuleman:

Boston Common Asset Management, LLC (Boston Common) is an asset manager serving investors concerned about the social and environmental impact as well as financial return of their investments. As of September 30, 2008, we managed approximately $900 million in-house and subadvised assets. Our clients are long term shareholders of AT&T common stock and currently hold 114,166 shares.

I am hereby authorized to notify you of our intention to co-file with Trillium Asset Management the enclosed shareholder resolution. Boston Common submits this shareholder proposal to AT&T for inclusion in the 2009 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities and Exchange Act of 1934 (17 C.F.R. § 240.14a-8). Per Rule 14a-8, our clients hold more than $2,000 of AT&T common stock, acquired more than one year prior to this date. Boston Common will continue to maintain at least $2,000 of AT&T through the date of the 2009 annual meeting. Verification of ownership from our custodian will be provided upon request. A representative of the shareholder group will attend the stockholders' meeting to move the shareholder proposal as required by the SEC rules.

Please direct any communications to Melissa Locke, at (617) 960-3920, or via email at mlocke@bostoncommonasset.com.

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

Sincerely,

Melissa K. Locke
Social Research & Advocacy Analyst

Cc: Jonas Kron, Trillium Asset Management

Report on Network Management Practices,
Public Expectations of Privacy and Freedom of Expression on the Internet

The Internet is becoming the defining infrastructure of our economy and society in the 21st century. Its potential to open markets for commerce, venues for cultural expression and modalities of civic engagement is without historic parallel.

Internet Service Providers (ISPs) are gatekeepers to this infrastructure: providing access, managing traffic, insuring communication, and forging rules that shape, enable and limit the public's Internet use.

As such, ISPs have a weighty responsibility in devising network management practices. ISPs must give far-ranging thought to how these practices serve to promote--or inhibit--the public's participation in the economy and in civil society.

Of fundamental concern is the effect ISPs' network management practices have on public expectations of privacy and freedom of expression on the Internet.

Whereas:

- More than 211 million Americans--70% of the population--use the Internet;
- The Internet serves as an engine of opportunity for social, cultural and civic participation in society;
- 46% of Americans have used the internet, e-mail or text messaging to participate in the 2008 political process;
- The Internet yields significant economic benefits to society, with online U.S. retailing revenues – only one gauge of e-commerce - exceeding $200 billion in 2008;
- The Internet plays a critical role in addressing societal challenges such as provision of health care, with over 8 million Americans looking for health information online daily;
- 72% of Americans are concerned that their online behaviors are being tracked and profiled by companies;
- 54% of Americans are uncomfortable with third parties collecting information about their online behavior;
- Our Company provides Internet access to a very large number of subscribers and is considered a leading ISP;
- Our Company's network management practices have been questioned by consumers, civil liberties groups and shareholders; specifically, AT&T was scrutinized for censoring political speech; was the focus of a BusinessWeek story discussing content monitoring; and was called before Congress to testify on these issues;

- Class action lawsuits in several states are challenging the propriety of ISPs' network management practices;

- Internet network management is a significant public policy issue; failure to fully and publicly address this issue poses potential competitive, legal and reputational harm to our Company;

- Any perceived compromise by ISPs of public expectations of privacy and freedom of expression on the Internet could have a chilling effect on the use of the Internet and detrimental effects on society.

Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet.

Supporting Statement

One example of an issue to be examined could be the social and political effects of collecting and selling personal information to third-parties, including information companies such as First Advantage and Equifax.

Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
208 S. Akard St., Room 3000.18
Dallas, Texas 75202
Ph. (214) 464-8815

November 14, 2008

Via UPS
Boston Common Asset Management, LLC
84 State Street, Suite 1000
Boston, MA 02109

Attn: Melissa K. Locke
Social Research & Advocacy Analyst

Dear Ms. Locke:

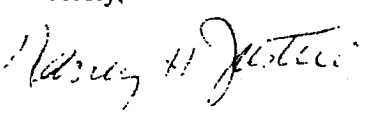
On November 11, 2008, we received your letter dated November 10, 2008, submitting a stockholder proposal for inclusion in the proxy materials for AT&T Inc.'s 2009 annual meeting. We are currently reviewing the proposal to determine if it is appropriate for inclusion.

Under the rules of the Securities and Exchange Commission ("SEC"), in order to be eligible to submit a stockholder proposal, a stockholder must: (a) be the record or beneficial owner of at least $2,000 in market value of shares of AT&T Inc. common stock at the time a proposal is submitted and (b) have continuously owned these shares for at least one year prior to submitting the proposal.

Boston Common Asset Management does not appear in our records as a registered stockholder. Therefore, in accordance with SEC rules, you must submit to us a written statement from the record holder of the shares (usually a broker or bank) verifying that, at the time the proposal was submitted, the requisite number of shares were continuously held for at least one year. *You must provide the required documentation no later than 14 days from your receipt of this letter.*

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

Sincerely,



BOSTON COMMON
ASSET MANAGEMENT

MEMORANDUM

Nancy Justice
Director SEC Compliance
4 ATT Center
311 S. Akard
Room 2-36
Dallas, TX 75202

RE: Shareholder Resolution Co-Filed With Trillium Asset Management

Ms. Justice –

On November 17, 2008 we received your letter dated November, 14, 2008 requesting a written statement from our record holder affirming the number of shares that Boston Common Asset Management held as of November 10, 2008, and which were held continuously for at least one year. Please find the requested statement attached.

Please call me at 617-916-3920 or Dawn Wolfe at 617-916-3915 if you have any questions.

Sincerely,

Melissa Locke
Boston Common Asset Management

STATE STREET.

Wealth Manager Services
Crown Colony Office Park
1200 Crown Colony Drive
Quincy, MA 02169

November 10, 2008

AT&T, Inc.
175 E. Houston
San Antonio, Texas 78205
Attention: Corporate Secretary

Dear Sir or Madam:

State Street is the custodian and record holder for Boston Common Asset Management.

We are writing to affirm that Boston Common Asset Management currently owns 38,064 shares of AT&T Inc. common stock, Omnibus Account BOSTONCOMMON. Boston Common Asset Management has beneficial ownership of at least one percent or $2,000 in market value of the voting securities of AT&T Inc. common stock and such beneficial ownership has existed for one or more years as of the filing date in accordance with rule 14a-8(a)(1) of the Securities Exchange Act of 1934, and that it will continue to hold the securities through the date of the 2009 annual meeting of shareholders.

Sincerely,

Lesley A. Lendh
Senior Associate
State Street WMS

November 7, 2008

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

Dear Sir or Madam,

Calvert Asset Management Company, Inc. ("Calvert"), a registered investment advisor, provides investment advice for the 42 mutual fund portfolios sponsored by Calvert Group, Ltd., including Calvert's 22 socially responsible mutual funds. Calvert currently has over $12.5 billion in assets under management.

The Calvert Social Investment Fund Balanced Portfolio, Calvert Variable Series, Inc. Calvert Social Balanced Portfolio, Calvert Social Investment Fund Enhanced Equity Portfolio, and Calvert Social Index Fund (together, the "Funds") are each beneficial owners of at least $2,000 in market value of securities entitled to be voted at the next shareholder meeting (supporting documentation available upon request). Furthermore, each Fund has held these securities continuously for at least one year, and it is Calvert's intention that the Funds continue to own shares in the Company through the date of the 2009 annual meeting of shareholders.

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

As a long-standing shareholder, we are filing the enclosed resolution requesting that the Board of Directors prepare a report discussing their network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet.

We understand that Jonas Kron on behalf of Trillium Asset Management is submitting an identical proposal. Calvert recognizes Trillium Asset Management as the lead filer and intends to act as a co-sponsor of the resolution. Mr. Kron has agreed to coordinate contact between the Corporation and other shareholders filing the proposal, including Calvert, and is also authorized to withdraw the resolution on Calvert's behalf. However, Calvert would like to receive copies of all correspondence sent to Mr. Kron as it relates to the proposal. In this regard,

A UNIFI Company.

4550 Montgomery Avenue
Bethesda, MD 20814
800.368.2748
www.calvert.com

Report on Network Management Practices,
Public Expectations of Privacy and Freedom of Expression on the Internet

The Internet is becoming the defining infrastructure of our economy and society in the 21st century. Its potential to open markets for commerce, venues for cultural expression and modalities of civic engagement is without historic parallel.

Internet Service Providers (ISPs) are gatekeepers to this infrastructure: providing access, managing traffic, insuring communication, and forging rules that shape, enable and limit the public's Internet use.

As such, ISPs have a weighty responsibility in devising network management practices. ISPs must give far-ranging thought to how these practices serve to promote--or inhibit--the public's participation in the economy and in civil society.

Of fundamental concern is the effect ISPs' network management practices have on public expectations of privacy and freedom of expression on the Internet.

Whereas:

- More than 211 million Americans--70% of the population--use the Internet;
- The Internet serves as an engine of opportunity for social, cultural and civic participation in society;
- 46% of Americans have used the internet, e-mail or text messaging to participate in the 2008 political process;
- The Internet yields significant economic benefits to society, with online U.S. retailing revenues -- only one gauge of e-commerce - exceeding $200 billion in 2008;
- The Internet plays a critical role in addressing societal challenges such as provision of health care, with over 8 million Americans looking for health information online daily;
- 72% of Americans are concerned that their online behaviors are being tracked and profiled by companies;
- 54% of Americans are uncomfortable with third parties collecting information about their online behavior;
- Our Company provides Internet access to a very large number of subscribers and is considered a leading ISP;
- Our Company's network management practices have been questioned by consumers, civil liberties groups and shareholders; specifically, AT&T was scrutinized for censoring political speech; was the focus of a BusinessWeek story discussing content monitoring; and was called before Congress to testify on these issues;

- Class action lawsuits in several states are challenging the propriety of ISPs' network management practices;

- Internet network management is a significant public policy issue; failure to fully and publicly address this issue poses potential competitive, legal and reputational harm to our Company;

- Any perceived compromise by ISPs of public expectations of privacy and freedom of expression on the Internet could have a chilling effect on the use of the Internet and detrimental effects on society.

Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet.

Supporting Statement

One example of an issue to be examined could be the social and political effects of collecting and selling personal information to third-parties, including information companies such as First Advantage and Equifax.

Sincerely,

Ivy Wafford Duke, Esq.
Assistant Vice President

Cc: Bennett Freeman, Senior Vice President for Social Research and Policy, Calvert Asset Management Company, Inc.

Stu Dalheim, Director, Shareholder Advocacy, Calvert Asset Management Company, Inc.

Aditi Vora, Social Research Analyst, Calvert Asset Management Company, Inc.

Enclosures: Resolution Text

Nancy H. Justice
Director – SEC Compliance
AT&T Inc.
208 S. Akard St., Room 3000.18
Dallas, Texas 75202
Ph. (214) 464-8815

November 12, 2008

Via UPS
Calvert Asset Management Company, Inc.
4550 Montgomery Avenue
Bethesda, MD 20814

Attn: Ivy Wafford Duke, Esq.
Assistant Vice President

Dear Ms. Duke:

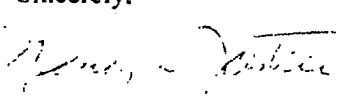
On November 11, 2008, we received your letter dated November 7, 2008, submitting a stockholder proposal for inclusion in the proxy materials for AT&T Inc.'s 2009 annual meeting. We are currently reviewing the proposal to determine if it is appropriate for inclusion.

Under the rules of the Securities and Exchange Commission ("SEC"), in order to be eligible to submit a stockholder proposal, a stockholder must: (a) be the record or beneficial owner of at least $2,000 in market value of shares of AT&T Inc. common stock at the time a proposal is submitted and (b) have continuously owned these shares for at least one year prior to submitting the proposal.

Calvert Asset Management Company does not appear in our records as a registered stockholder. Therefore, in accordance with SEC rules, you must submit to us a written statement from the record holder of the shares (usually a broker or bank) verifying that, at the time the proposal was submitted, the requisite number of shares were continuously held for at least one year. *You must provide the required documentation no later than 14 days from your receipt of this letter.*

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

Sincerely,



Calvert
INVESTMENTS
THAT MAKE A DIFFERENCE®

November 20, 2008

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

Dear Sir or Madam,

I am writing in response to your November 12, 2008 letter to Ivy Wafford Duke regarding the stockholder proposal submitted by Calvert Asset Management Company, Inc.

Please see the enclosed letter documenting that the Calvert Social Investment Fund Balanced Portfolio, Calvert Variable Series, Inc. Calvert Social Balanced Portfolio, Calvert Social Investment Fund Enhanced Equity Portfolio, and Calvert Social Index Fund each held more than $2,000 in market value of AT&T Inc. common stock as of close of business on November 7, 2008 when Calvert submitted its shareholder proposal, and that each of these funds has continuously held these shares for at least one year prior to the date we submitted the proposal.

Please contact me immediately by phone at (301)-961-4715 or email aditi.vora@calvert.com if you have any further questions regarding this matter.

Sincerely,

Aditi Vora
Social Research Analyst

Enclosures: State Street Letter

Cc: Nancy Justice, Director- SEC Compliance, AT&T Inc.

Stu Dalheim, Director, Shareholder Advocacy, Calvert Asset Management Company, Inc.

A UNIFI Company

4550 Montgomery Avenue
Bethesda, MD 20814
800.368.2748
www.calvert.com

STATE STREET

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

November 19, 2008,

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

To Whom It May Concern:

This letter is to confirm that as of November 7, 2008 the Calvert Funds listed below held the indicated amount of shares of the stock of AT&T, INC. (CUSIP 00206R102). Also the funds held the amount of shares indicated continuously for one year.

Fund Number	Name	Shares as of 11/07/08	Shares held for 1 year
D805	CSIF Balanced Portfolio	305,075	259,565
D835	CVS Calvert Social Balanced Portfolio	231,900	208,977
D862	CSIF Enhanced Equity Portfolio	78,442	76,242
D872	Calvert Social Index Fund	98,338	67,408
D874	Calvert Large Cap Growth Fund	401,500	0

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

Sincerely,

Michelle McElroy
Account Manager
State Street Corp

ANNEX B

AT&T Privacy Policy

AT&T Privacy Notice

Effective 06/16/06

OUR COMMITMENT: RESPECTING AND PROTECTING YOUR PRIVACY

Back to Privacy Summary

OUR COMMITMENT: RESPECTING AND PROTECTING YOUR PRIVACY

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

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

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

We have a long history of vigorously protecting customer and web visitor privacy. Our customers and web visitors expect, deserve and receive nothing less than our fullest commitment to their privacy. We also have an obligation to assist law enforcement and other government agencies responsible for protecting the public welfare, whether it be an individual or the security interests of the entire nation. If and when we are asked to help, we do so strictly within the law and under the most stringent conditions.

* AT&T Inc. was created on Nov. 18, 2005, through a merger of SBC Communications Inc. and AT&T Corp. We continue to undergo branding changes to bring together all former SBC and AT&T brands and this privacy policy applies irrespective of AT&T or SBC branding.

top

THE SCOPE OF THIS PRIVACY POLICY

This privacy policy addresses the privacy of AT&T retail customers and Web visitors in the United States. Where applicable, AT&T will comply with the laws of other countries that contain mandatory requirements that differ from this policy. In selected jurisdictions outside the United States, a member of the AT&T family of companies may adopt a separate privacy policy to reflect the requirements of applicable local laws.

This policy identifies the types of data and information we collect, how we use it, how you can control its use and the steps we take to protect it. The primary focus of this policy is non-public information that identifies or

that is linked to the identity of a customer or Web visitor ("personal identifying information").

In this policy, the AT&T family of companies means AT&T Inc. and its subsidiary and affiliated entities. Members of the AT&T family of companies have agreed to the privacy practices in this policy — except for Wireless from AT&T, formerly Cingular® Wireless and YELLOWPAGES.COM, both of which are joint ventures between AT&T and Bell South and operate under their own privacy policies. Personal identifying information shared between Wireless from AT&T, formerly Cingular® Wireless or YELLOWPAGES.com and other AT&T family of company members will be used and protected as set forth in this policy.

This policy does not apply where non-members of the AT&T family of companies ("third parties") have licensed the AT&T brand for use with their own products or services. For example, the policy does not apply to Advanced American Telephones, which licenses the AT&T Brand to sell telephone equipment, or to Citibank, which licenses the AT&T Brand to offer its AT&T Universal Card.

When you sign up for certain AT&T-offered services, you may agree to additional privacy policies that address service-specific privacy practices. For example, certain AT&T Internet services — AT&T Dial, AT&T High Speed Internet, and AT&T High Speed Internet U-verse Enabled — and AT&T U-verse TV and Homezone services are subject to an additional privacy policy. View a copy of the AT&T Internet Service and Video Services policy. Similarly, AT&T | DISH network service is subject to an additional privacy policy.

top

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

Personal identifying information we collect and use

We collect personal identifying information regarding our customers, including information customers give us, information collected as a result of the customer's relationship with us and information we obtain from other sources. Examples include name; address; e-mail address; telephone number; billing, payment, usage, credit and transaction information (including credit card numbers, account numbers and/or social security number); and demographic information.

We also collect personal identifying information that our Web visitors choose to provide to us (e.g., name, address, telephone number, e-mail address) when registering on our Web sites; ordering AT&T-offered products or services; sending us e-mail; responding to our surveys; entering contests or sweepstakes; or in connection with online ordering or billing functions.

We use the personal identifying information of a customer to provide, confirm, change, bill, monitor and resolve problems with the quality of AT&T-offered products and services. We also use the personal identifying information of a customer or Web visitor to develop, market and sell our products and services.

We may aggregate the personal identifying information of different customers or Web visitors to produce data about a group or category of services, customers or Web visitors. For example, we might use aggregate data about the types of services our customers have generally purchased at the same time in order to develop attractive bundled service offerings. Such aggregate data, however, will not reflect any personal identifying information of any specific customer or Web visitor.

Personal identifying information we disclose to third parties

We do not provide personal identifying information (other than information included in our directories and directory assistance service) to third parties for the marketing of their products and services without your consent.

We may provide personal identifying information to third parties where required to provide certain AT&T-offered products and services. For example, we disclose certain AT&T | DISH Network-related personal identifying information to Echostar Satellite Corporation, L.L.C. and its affiliates solely in order to provide AT&T | DISH Network services.

We may also provide personal identifying information to third parties who perform functions or services on our behalf. Examples include shipping companies who deliver AT&T products; AT&T-authorized agents who market and sell AT&T-offered products and services on our behalf; and Web site development or advertising companies, who provide Web design, analysis and advertising services.

When we provide such personal identifying information to third parties to perform such functions or services on our behalf, we require that they protect personal identifying information consistent with this policy and do not allow them to use such information for other purposes.

We may, where permitted or required by law, provide personal identifying information to third parties (including credit bureaus or collection agencies) without your consent:

To obtain payment for AT&T-offered products and services, enforce or apply our customer agreements, and/or protect our rights or property.

To comply with court orders, subpoenas, or other legal or regulatory requirements.

To prevent unlawful use of communications or other services, to assist in repairing network outages, and when a call is made to 911 from a customer phone and information regarding the caller's location is transmitted to a public safety agency.

To notify a responsible governmental entity if we reasonably believe that an emergency involving immediate danger of death or serious physical injury to any person requires or justifies disclosure without

delay.

A customer's name and telephone number may also be transmitted and displayed on a Caller ID device unless the customer has elected to block such information. Caller ID Blocking does not prevent the display of the number when you dial certain business numbers, 911, 900 numbers or toll-free 800, 888, 877 or 866 numbers.

Information included in our directories and directory assistance service

We publish and distribute directories in print, on the Internet, and on CDs and/or other electronic media (some complimentary and some for a fee). These directories include limited personal identifying information about our customers — i.e., published customer names, addresses and telephone numbers — without restriction to their use. Our directories may also include information obtained from third parties. We also make that information available through directory assistance operators and through the Internet. For more information on controlling the disclosure of this information, see Obtaining non-published and non-listed numbers below.

We are required by law to provide published customer names, addresses and telephone numbers (or non-published status) to unaffiliated directory publishers and directory assistance providers, over whom AT&T has no control, for their use in creating directories and offering directory assistance services.

This directory information is not legally protected by copyrights and may be sorted, packaged, repackaged and made available again in different formats by anyone, including AT&T.

Obtaining non-published and non-listed numbers

Except as described below, telephone listings of AT&T local telephone customers are made available in our directories and through directory assistance.

When a customer subscribes to AT&T local telephone service, we offer the opportunity to request that the customer's name, number, and address not be published in our directories or made available through our directory assistance.

The names, numbers and addresses of customers who choose to have a "non-published" number will not be available in our directories or through our directory assistance. Likewise, we do not make non-published numbers available to others to include in directories or to provide directory assistance services.

The names, numbers and addresses of customers who choose to have a "non-listed" number will not be available in AT&T directories, but the information will be publicly available through directory assistance and will be provided to unaffiliated directory assistance providers over whom AT&T exercises no control.

There is a fee for customers who choose to have non-published or non-listed telephone numbers.

Customers may choose to exclude partial or all address information from their listings.

Customers in Nevada do not have the option of a non-listed number.

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

Our "Do Not Call" lists

We comply with all applicable laws and regulations regarding "Do Not Call" lists. These laws generally permit companies to contact their own customers even though such customers are listed on the federal and, in some instances, state "Do Not Call" lists.

Residential consumers may request that they be removed from AT&T's telemarketing lists at any time, including when an AT&T marketing and promotional call is received or by contacting an AT&T service representative.

Where required by state laws and/or regulations, we also honor requests from business customers to be removed from our telemarketing lists.

Wireless from AT&T, formerly Cingular® Wireless maintains its own "Do Not Call" policy and lists. Please contact Wireless from AT&T, formerly Cingular Wireless directly at 1-866-CINGULAR if you wish to be placed on its "Do Not Call" list.

Customer Proprietary Network Information

In the normal course of providing telecommunications services to our customers, we collect and maintain certain customer proprietary network information, also known as "CPNI". Your CPNI includes the types of telecommunications services you currently purchase, how you use them and related billing information for those services. Your telephone number, name and address are not CPNI.

Protecting the confidentiality of your CPNI is your right and our duty under federal law. We do not sell, trade or share your CPNI — including your calling records — with anyone outside of the AT&T family of companies or with anyone not authorized to represent us to offer our products or services, or to perform functions on our behalf except as may be required by law or authorized by you.

As a general rule, we are permitted to use CPNI in our provision of telecommunications services you purchase, including billing and collections for those services. We are permitted to use or disclose CPNI to offer telecommunications services of the same type that you already purchase from us. We may also use or disclose your CPNI for legal or regulatory reasons such as a court order, to investigate fraud or to protect

against the unlawful use of our telecommunications network and services and to protect other users.

Click here for more information on the use of CPNI.

top

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

Web usage information we collect and use

When Web visitors access our Web sites we automatically receive certain "Web usage" information. For example, our Web servers automatically collect the visitor's IP address, the visitor's Web browser and operating system types, and the identity of the Web page from which the visitor's browser entered our Web site. In addition, primarily through the use of cookies or Web beacons, we may collect other Web usage information, such as the Web pages the browser visits on our Web sites, the amount of time spent on such Web pages and whether the browser re-visits our Web sites/pages.

We use Web usage information to facilitate and enable the functioning of our Web sites and to expand and improve our Web visitors' online experience. We may also aggregate such Web usage information with other visitors' Web usage information to assess trends and better design, monitor and otherwise improve our Web sites, as well as to focus our marketing efforts.

In some cases we may combine Web usage information related to your access to our Web sites with personal identifying information. We use the combined information to provide our customers and Web visitors with a better online experience by providing customized features and services and to market and provide advertising about goods and services that may be of particular interest. Once combined, the resulting data is protected as personal identifying information as described in this policy.

How we use cookies, Web beacons, etc.

Cookies are alphanumeric identifiers that a Web server sends to your computer when you visit a Web site. Cookies can contain a variety of information, such as a simple count of how often you visit a Web site or information that allows us to customize our Web site for your use. Web beacons (also known as "clear gifs" or "one-pixel gifs") are small graphic images on a Web page or in an e-mail that allow us to monitor the activity on our Web sites or to make cookies more effective.

We, or a third party acting on our behalf, may use "cookies" to tailor and improve the content we deliver to our Web visitors, to improve our Web sites by assessing which areas, features, and products are most popular, and to personalize our Web sites and make recommendations based on information, including product choices, a particular visitor has previously provided. For example, we may use a cookie to identify your state so we do not ask you to enter it more than once. We also use cookies to store user preferences, complete online order activity and keep track of transactions.

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

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

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

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

Our e-mail marketing practices

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

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

Our policy on online access by children

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

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

We comply with all applicable laws and regulations, including the Children's Online Privacy Protection Act

(COPPA), which requires the consent of a parent or guardian for the collection of personally identifiable information from children under 13.

Linking to other sites

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

Online privacy education

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

top

HOW WE PROTECT YOUR INFORMATION

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

We employ security measures designed to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data, including personal identifying information. We have implemented technology and security features and strict policy guidelines to safeguard the privacy of your personal identifying information, and we will continue to enhance our security procedures as new technology becomes available. For example:

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

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

top

PRIVACY POLICY UPDATES

This privacy policy supersedes and replaces all previously posted privacy policies.

We want you to be aware of the information we collect, how we use it and under what circumstances, if any, we disclose it. We reserve the right to update this privacy policy to reflect any changes we make in order to continue to serve the best interests of our customers and Web visitors and will timely post those changes. If we make a material change to this privacy policy, we will post a prominent notice on our Web sites.

If we intend, however, to use personal identifying information in a manner materially different from that stated at the time of collection, we will attempt to notify you at least 30 days in advance using an address or e-mail address, if you have provided one, and by posting a prominent notice on our Web sites, and you will be given a choice as to whether or not we use your information in this different manner.

Please periodically check our Web sites for changes to this privacy policy.

top

CONTACTING US: QUESTIONS, COMMENTS, CONCERNS

AT&T honors requests from customers and Web visitors to review their personal identifying information that we maintain in reasonably retrievable form and we will gladly correct any such information that is inaccurate. You may verify that appropriate corrections have been made. Please contact an AT&T service representative.

If you are receiving unwanted e-mails at or from an SBC Internet Service e-mail address (e.g., @sbcglobal.net, @yahoo.com) please visit the AT&T Yahoo! Anti-Spam Resource Center. For AT&T Worldnet unwanted e-mails, please visit the AT&T Worldnet Spam Center.

We are happy to address any concerns you may have about our privacy practices and policies. You may e-mail us at privacypolicy@ATT.com or write to us at AT&T Privacy Policy, 175 E. Houston St., San Antonio, TX 78205.

AT&T is a TRUSTe licensee. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence in the Internet by promoting the use of fair information practices. Because AT&T wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and

have its privacy practices reviewed for compliance by TRUSTe. The TRUSTe program covers only information collected through AT&T Web sites, and does not cover information that may be collected through software downloaded from such sites.

AT&T's privacy policy and practices also meet the requirements of the Better Business Bureau's Online Privacy Program, and we proudly display the BBBOnLine Privacy Seal. Further information about this program is available at www.bbbonLine.org.

If you have questions or concerns regarding this policy, you should first contact us via e-mail at privacypolicy@att.com. If you do not receive acknowledgment of your inquiry or your inquiry is not satisfactorily addressed, you should then contact TRUSTe through the TRUSTe Watchdog Dispute Resolution Process and TRUSTe will serve as a liaison to resolve your concerns. You may also contact BBBOnLine at www.bbbonLine.org.

top

ANNEX C

Statement of Dorothy Attwood

STATEMENT OF DOROTHY ATTWOOD
SENIOR VICE PRESIDENT, PUBLIC POLICY & CHIEF PRIVACY OFFICER
AT&T INC.

BEFORE:

UNITED STATES SENATE
COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

HEARING ON BROADBAND PROVIDERS AND CONSUMER PRIVACY

September 25, 2008

Thank you, Chairman Inouye and Ranking Member Hutchison, for providing AT&T Inc. the opportunity to discuss online advertising and, more specifically, the issue that has received a good deal of recent attention, so-called online behavioral advertising. We trust that this hearing will help the discussion evolve past slogans and rhetoric to a more thoughtful examination of the facts and the development of a holistic consumer privacy policy framework that all participants in the online behavioral advertising sphere can and will adopt.

Your interest in these matters surely is warranted. Online advertising fuels investment and innovation across a wide range of Internet activities, and provides the revenue that enables consumers to enjoy many free and discounted services. Likewise, website publishers make most of their money from advertising, which revenue in turn funds today's vast wealth and diversity of Internet content and information – most of which consumers enjoy, again, for free. On the other hand, online advertising, especially next-generation forms of highly targeted behavioral advertising that involve tracking consumer web browsing and search activities, raise important consumer-privacy concerns that policymakers and industry must carefully weigh. In short,

setting proper policy in this area will be crucial to a healthy and growing Internet ecosystem that benefits consumers.

AT&T does not today engage in online behavioral advertising, but we understand the uniquely sensitive nature of this practice. We have listened to our customers and watched the debate unfold, and are responding by advocating for a consumer-focused framework. As described in more detail herein, the pillars of this framework – *transparency, consumer control, privacy protection, and consumer value* – can be the foundation of a consistent regime applicable to all players in the online behavioral advertising sphere – including not just Internet Service Providers ("ISPs"), but also search engines and third party advertising networks – that both ensures that consumers have ultimate control over the use of their personal information and guards against privacy abuses.[1]

In particular, we believe that effective customer control for online behavioral advertising requires meaningful consent and therefore commit that *AT&T will not use consumer information for online behavioral advertising without an affirmative, advance action by the consumer that is based on a clear explanation of how the consumer's action will affect the use of her information.* This concept – often generically referred to as "opt-in" – means that a consumer's failure to act will *not* result in any collection and use by default of that consumer's information for online behavioral advertising purposes. This affirmative consent model differs materially from the default-based privacy policies that advertising networks and search engines – which already are

[1] The policy framework that AT&T proposes here is informed by and should complement the Online Behavioral Advertising Self-Regulatory Principles issued by staff of the Federal Trade Commission in December of last year. Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, available at http://www.ftc.gov/05/2007/12/P85900stmt.pdf.

engaged in online behavioral advertising – currently employ. Given the obvious consumer benefits of such a model, we encourage all companies that engage in online behavioral advertising – regardless of the nature of their business models or the technologies they utilize – likewise to adopt this affirmative-advance-consent paradigm.

What is Online Behavioral Advertising?

There is no single, settled definition of online behavioral advertising in statute or case law, but the FTC and others have used the term to refer to it as the tracking of a consumer's web search and web browsing activities – by tracking either the person or a particular Internet access device, be it a computer, data-enabled mobile phone, or some other communications vehicle – to create a distinct profile of the consumer's online behavior. In this sense, it can clearly be distinguished from the simple practice of tracking a consumer's use of an individual website or obviously-related websites (such as those operated under a common trademark, trade name or conspicuously disclosed corporate affiliation), which practice does not necessarily raise the same privacy concerns as online behavioral advertising but which nonetheless can and should expressly be disclosed to Internet users. Privacy concerns about online behavioral advertising are not new – indeed, DoubleClick's (now a Google subsidiary) use of tracking cookies to collect and use information about consumer web browsing activity was the subject of an FTC proceeding in 2000.[2] More recently, the FTC and Congress have appropriately asked questions about the privacy implications of emerging online advertising businesses that involve the tracking of consumer web browsing and search activity. Thus, consistent with the focus of recent public discussion, we consider online behavioral advertising to be (1) the tracking of user

[2] Letter from Joel Winston, Acting Associate Director, Division of Financial Practices, Bureau of Consumer Protection, Federal Trade Commission, to ChristineVarney, Hogan & Hartson, Re: DoubleClick Inc. (Jan 22, 2001)(memorializing closure of FTC staff investigation).

web browsing and search activity across unrelated websites, (2) when the tracking and association of the websites or their components are largely invisible to the user, and (3) the resulting information is used to create a distinct user profile and deliver targeted advertising content.

Online behavioral advertising can take many forms. It can, for instance, involve the use by an ISP of technologies to capture and analyze a user's Internet browsing activities and experience across unrelated websites. These more ISP-specific methodologies are not, however, the only – and certainly are not nearly the most prevalent – forms of online behavioral advertising. Advertising-network technologies have evolved beyond solely tracking consumer web surfing activity at sites on which they sell advertising. They now also have the ability to observe a user's entire web browsing experience at a granular level. Techniques include the ad network "dropping" third-party tracking "cookies" on a consumer's computer to capture consumer visits to any one of thousands of unrelated websites; embedding software on PCs; or automatically downloading applications that – unbeknownst to the consumer – log the consumer's full session of browsing activity.

Ad networks and other non-ISPs employ these capabilities at the individual browser or computer level and they are as effective as any technique that an ISP might employ at creating specific customer profiles and enabling highly targeted advertising. Already ad networks and search engines track and store a vast trove of data about consumers' online activities. Google's practices exemplify the already extensive use of online behavior advertising, particularly by non-ISPs. Google logs and stores users' search requests, can track the search activity by IP address

and a cookie that identifies the user's unique browser, and can even correlate search activities across multiple sessions, leading to the creation of a distinct and detailed user profile. Through DoubleClick, Google can drop tracking cookies on consumers' computers so that whenever the consumer visits web sites that contain a display ad placed by DoubleClick (which can be for virtually any product or service), the consumer's web browsing activity can be tracked across seemingly unrelated sites (e.g., CNN.com or ESPN.com). Google further has access to enormous amounts of personal information from its registered users, which its privacy policy expressly confirms can be combined with information from other Google services or third parties for the "display of customized content and advertising." And it even scans emails from non-Gmail subscribers sent to Gmail subscribers for contextual advertising purposes.

Thus, if anything, the largely invisible practices of ad-networks and search engines raise at least the same privacy concerns as do the online behavioral advertising techniques that ISPs could employ, such as deep-packet-inspection, which have application beyond mere targeted advertising, including managing network congestion, detecting viruses and combating child pornography. In short, the privacy and other policy issues surrounding online behavioral advertising are not technology-specific. The relevant touchstones are the manner in which consumer information is tracked and used, and the manner in which consumers are given notice of and are able to consent to or prohibit such practices. Those factors are entirely technology-neutral.

AT&T's Approach to Online Behavioral Advertising

AT&T does not today engage in online behavioral advertising.[3] This is not because AT&T sees no value in this next-generation form of online advertising. Indeed, if done properly, online behavioral advertising could prove quite valuable to consumers and could dramatically improve their online experiences. We do, however, believe it is essential to include strong privacy protections in the design of any online behavioral advertising program, which is why we will initiate such a program only after testing and validating the various technologies and only after establishing clear and consistent methods and procedures to ensure the protection of, and ultimate consumer control over, consumer information. We further intend to work with privacy advocates, consumer privacy coalitions and fellow industry participants in a cooperative, multi-faceted effort that we trust can and will lead to a predictable consumer driven framework in this area. In any event, if AT&T deploys these technologies and processes, it will do so the right way.

Against this backdrop, AT&T has already listened closely to its customers and will adopt meaningful and flexible privacy principles that will guide any effort to engage in online behavioral advertising. We summarize this framework as follows:

---

[3] AT&T does engage in some of the more ordinary and established aspects of online advertising. Like virtually every entity with a retail Internet presence, AT&T tracks usage on its own websites, such as att.com, in order to improve the online experience, optimize a particular site's capabilities and ease-of-use, and provide the most useful information to consumers about AT&T's products and services. In addition, like thousands of other businesses that operate websites, AT&T does business with advertising networks and has partnered with providers of online search. For example, on the AT&T broadband Internet access portal, AT&T makes space available for advertising provided by the Yahoo! advertising network, and users of the portal may be shown advertising that is based on their activity across sites signed up to the Yahoo! advertising network. Also by way of example, we have arranged for the Google search box to appear on our my.att.net site. In this regard, then, we are no different than any other website publisher.

- ***Transparency:*** Consumers must have full and complete notice of what information will be collected, how it will be used, and how it will be protected.

- ***Consumer Control:*** Consumers must have easily understood tools that will allow them to exercise meaningful consent, which should be a sacrosanct precondition to tracking online activities to be used for online behavioral advertising.

- ***Privacy protection:*** The privacy of consumers/users and their personal information will be vigorously protected, and we will deploy technology to guard against unauthorized access to personally identifiable information

- ***Consumer Value:*** The consumer benefits of an online behavioral advertising program include the ability to receive a differentiated, secure Internet experience that provides consumers with customized Internet advertisements that are relevant to their interests. But we think the future is about much more than just customized advertising. Consumers have shown that in a world of almost limitless choices in the content and services available on the Internet, they see great value in being able to customize their unique online experience. That is the ultimate promise of the technological advances that are emerging in the market today.

Call to Action

We believe these principles offer a rational approach to protecting consumer privacy while allowing the market for Internet advertising and its related products and services to grow. But, in order for consumers truly to be in control of their information, *all* entities involved in Internet advertising, including ad networks, search engines and ISPs, will need to adhere to a consistent set of principles. A policy regime that applies only to one set of actors will arbitrarily favor one business model or technology over another and, more importantly, represent only a partial and entirely unpredictable solution for consumers. After all, consumers do not want information and control with respect to just a subset of potential online advertising or the tracking and targeting that might underlie those ads. Thus, we urge all entities that engage in online behavioral advertising – including especially those who already engage in the practice – to join AT&T in committing to a policy of advance, affirmative consumer consent.

TRILLIUM ASSET MANAGEMENT®
25 Years of Investing for a Better World®

Trillium Asset Management Corporation
www.trilliuminvest.com

January 9, 2008

VIA e-mail: shareholderproposals@sec.gov

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

Re: Shareholder Proposal Submitted to AT&T Inc. for 2009 Proxy Statement

Dear Sir/Madam:

This letter is submitted on behalf of Jane Brown, Trillium Asset Management Corporation, Calvert Asset Management Company, Inc. and Boston Common Asset Management (hereinafter referred to as "Proponents"), who are beneficial owners of shares of common stock of AT&T Inc. (hereinafter referred to as "AT&T" or the "Company"), and who have jointly submitted a shareholder proposal (hereinafter referred to as "the Proposal") to AT&T, to respond to the letter dated December 10, 2007 sent to the Office of Chief Counsel by the Company, in which AT&T contends that the Proposal may be excluded from the Company's 2009 proxy statement by virtue of Rules 14a-8(i)(7) and 14a-8(i)(10).

I have reviewed the Proponents' shareholder proposal, as well as the Company's letter and supporting materials, and based upon the foregoing, as well as upon a review of Rule 14a-8, it is my opinion that the Proposal must be included in AT&T's 2009 proxy statement, because (1) the subject matter of the Proposal transcends the ordinary business of the Company by focusing on a significant social policy issue and (2) the requested report is not moot. Therefore, we respectfully request that the Staff not issue the no-action letter sought by the Company.

Pursuant to Staff Legal Bulletin 14D.C. a copy of these materials is being e-mailed concurrently to AT&T's counsel, Mr. David B. Harms at harmsb@sullcrom.com and Mr. Alexander Rakosi at rakosia@sullcrom.com.

Summary Response

As demonstrated below, a widespread public debate has developed about the role of Internet Service Providers ("ISPs") as gatekeepers to our civil liberties. As the proverbial "public square" has moved onto the Internet, the Internet management practices of ISPs have taken center stage in debates about free speech and public expectations of privacy. As more of our economic, social, political and cultural activities have moved online, ISPs are faced with new and profound questions about how to reconcile their roles as for-profit public companies with their responsibilities as content providers, news outlets, and protectors of public discourse and personal data. Shareholders are rightly concerned about the strategic and societal implications of these developments.

BOSTON	DURHAM	SAN FRANCISCO	BOISE
711 Atlantic Avenue	353 West Main Street, Second Floor	369 Pine Street, Suite 711	950 W. Bannock Street, Suite 530
Boston, Massachusetts 02111-2809	Durham, North Carolina 27701-3215	San Francisco, California 94104-3310	Boise, Idaho 83702-6118
T: 617-423-6655 F: 617-482-6179	T: 919-688-1265 F: 919-688-1451	T: 415-392-4806 F: 415-392-4535	T: 208-387-0777 F: 208-387-0278
800-548-5684	800-853-1311	800-933-4806	800-567-0538

AT&T's management seeks to deny shareholders the opportunity to consider these issues at the Company's annual meeting by arguing that the Proposal focuses on mundane matters and is substantially implemented by the Company's privacy policy and public statements. As demonstrated below, the Proposal focuses on an issue that has received significant attention from regulators, Congress and the press. We also demonstrate how the Company recognizes the significant public challenges posed by the issues. Finally, the following sections provide specific examples of where the Company has failed to implement the Proposal.

We therefore respectfully request the Staff to conclude that AT&T has failed to meet its burden of persuasion and cannot exclude the Proposal from its 2009 proxy materials.

The Proposal

Report on Network Management Practices,
Public Expectations of Privacy and Freedom of Expression on the Internet

The Internet is becoming the defining infrastructure of our economy and society in the 21st century. Its potential to open markets for commerce, venues for cultural expression and modalities of civic engagement is without historic parallel.

Internet Service Providers (ISPs) are gatekeepers to this infrastructure: providing access, managing traffic, insuring communication, and forging rules that shape, enable and limit the public's Internet use.

As such, ISPs have a weighty responsibility in devising network management practices. ISPs must give far-ranging thought to how these practices serve to promote--or inhibit--the public's participation in the economy and in civil society.

Of fundamental concern is the effect ISPs' network management practices have on public expectations of privacy and freedom of expression on the Internet.

Whereas:

- More than 211 million Americans--70% of the population--use the Internet;
- The Internet serves as an engine of opportunity for social, cultural and civic participation in society;
- 46% of Americans have used the Internet, e-mail or text messaging to participate in the 2008 political process;
- The Internet yields significant economic benefits to society, with online U.S. retailing revenues – only one gauge of e-commerce - exceeding $200 billion in 2008;
- The Internet plays a critical role in addressing societal challenges such as provision of health care, with over 8 million Americans looking for health information online daily;
- 72% of Americans are concerned that their online behaviors are being

tracked and profiled by companies;

- 54% of Americans are uncomfortable with third parties collecting information about their online behavior;
- Our Company provides Internet access to a very large number of subscribers and is considered a leading ISP;
- Our Company's network management practices have been questioned by consumers, civil liberties groups and shareholders; specifically, AT&T was scrutinized for censoring political speech; was the focus of a BusinessWeek story discussing content monitoring; and was called before Congress to testify on these issues;
- Class action lawsuits in several states are challenging the propriety of ISPs' network management practices;
- Internet network management is a significant public policy issue; failure to fully and publicly address this issue poses potential competitive, legal and reputational harm to our Company;
- Any perceived compromise by ISPs of public expectations of privacy and freedom of expression on the Internet could have a chilling effect on the use of the Internet and detrimental effects on society.

Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy and freedom of expression on the Internet.

Supporting Statement

One example of an issue to be examined could be the social and political effects of collecting and selling personal information to third-parties, including information companies such as First Advantage and Equifax.

Background

A plain reading of the Proposal makes it evident that it is about addressing the negative impacts of AT&T's business activities on freedom of speech and public expectations of privacy. It is not about the so-called warrantless wiretapping program and it is not about government surveillance. As much as the Company would like this case to be considered a re-play of the 2007 and 2008 proposals filed by As You Sow and does its best to paint the Proposal in that light, in reality the Proposal and the context from which it springs are substantially and fundamentally different from the As You Sow proposals. This Proposal focuses on threats to public expectations of privacy and freedom of expression from private/commercial interests.

The Proposal is distinct from the As You Sow proposals in how it addresses the issue of privacy. The As You Sow proposals focused on privacy policies, customer privacy and

government The Proposal, in contrast, is focused on the impact of the Company's Internet network management practices on public expectations of privacy – i.e. focusing on the social impact of the company's actual conduct. These are two very different subject matters, as discussed further below, which AT&T is attempting to conflate. The Company admits as much on Page Four of its letter when it acknowledges that there is no mention whatsoever of the warrantless wiretapping controversy in the Proposal and is left to resort to bald speculation about the Proponents' motivations. By doing so the Company is asking the Staff to ignore the text of the Proposal and engage in a baseless attempt to assess the Proponents' intentions. This is not the role of the Staff and is at odds with Staff practice.

Contrary to the Company's assertions, this Proposal does not originate in the shadows surrounding the warrantless wiretapping program. Rather, it stems from the controversial and widely publicized actions of AT&T in squelching the voice of Eddie Vedder, lead singer of one of the most popular music groups in the world. On August 5, 2007, AT&T censored its webcast of a performance by the rock band Pearl Jam, blocking the audio feed when Eddie Vedder ad-libbed some non-obscene but politically pointed lyrics:

> "George Bush, leave this world alone."
> "George Bush find yourself another home."

AT&T did not voluntarily disclose the fact of the censorship or the reasons for it until public attention was brought to the incident in the media. When confronted, AT&T blamed an overzealous sub-contractor and admitted to a "handful" of similar incidents of censorship.

A few days later, Trillium engaged AT&T management in dialogue on this issue. The Company disclosed that subsequent to the Pearl Jam episode it had adopted a "new policy" regarding censorship, but that policy apparently applies only to similar web performances. In as series of correspondence between AT&T and Trillium (five letters in all), the Company would not say how the First Amendment is being treated in other service offerings where AT&T functions as a content provider. See Exhibit A.

In a March 2008 letter to Trillium, AT&T said: "As the nation's largest provider or broadband services, we recognize our responsibility to protect our customers' freedom of expression on the Internet. In this dynamic environment, we must vigilantly and continually monitor and update our policies to ensure that they remain faithful to our overall vision."

However, AT&T would not provide Trillium with a copy of its freedom of speech policies. Left without other options, Trillium decided to exercise its rights as a shareholder to bring the issue of censorship before fellow shareholders at the Company's 2009 annual meeting.

In the course of developing the Proposal, Trillium consulted with a number of other shareholders and discovered that civil liberties issues presented by the Pearl Jam incident were both more widespread (extending to many ISPs other than AT&T) and more complex (with the issues of freedom of expression and privacy inextricably joined together).

As discussed below, a number of ISPs have been accused of engaging in censorship in very public ways – see. for example. Verizon's censorship of NARAL for "controversial material." For that reason, an identical proposal has been filed by the Proponents and other shareholders with Charter, Embarq, Verizon, CenturyTel, Sprint, Knology, Comcast and Qwest. The vast majority of these companies have no involvement whatsoever with the warrantless wiretapping controversy. While the Company may wish this Proposal to focus on that subject, it clearly does not.

It was also evident to us that freedom of speech issues are inextricably linked to consideration of public expectations of privacy on the Internet. The point here is that the Proposal explicitly **does not focus on AT&T's customers** – which was the subject of the As You Sow proposals. Rather, it addresses the impact AT&T's network management practices have on a much larger community. The free flow of traffic on the Internet is dependent on an industry practice known as "peering" – by which traffic is automatically transferred from one ISP to another; that means any individual ISP frequently carries data and content originating from, or destined for, virtually any Internet user in the world – whether or not those users are customers of the ISP. If people do not feel free to speak freely and anonymously online, then they may self-censor and not speak freely.

In short, the Proposal is categorically different from the As You Sow proposals. It stems from a censorship issue, it focuses on how the Company impacts society and, lastly, it is not focused on government activity. The As You Sow proposals were directly and clearly focused on the relationship between telecommunications companies and the government. This current Proposal is explicitly not focused on the government, but rather is focused on the commercial pressures on ISPs that threaten harm to society. In that sense it fits within the traditional model of environmental and human rights proposals that seek to minimize or eliminate the harmful impacts of company activities on the environment and human rights.

Finally, the As You Sow proposals were excluded for reasons not relevant to the Proposal. First, the 2007 AYS proposal was excluded for focusing on "litigation strategy" for requesting "past expenditures on attorney's fees." There is nothing in the Proposal that even remotely relates to the Company's litigation strategy. Second, the 2008 AYS Proposal was excluded for focusing on "procedures for protecting customer information" because it was explicitly focused on customer privacy. As discussed above and in the following sections, the Proposal does not run afoul of this exclusion both because it focuses on societal impacts as well as the civil liberties issues presented by public expectations of privacy and censorship.

The Proposal focuses on a significant 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 & Co.*, 958 F. 2d 416 (DC Cir. 1992) a proposal may not be excluded if it has "significant policy, economic or other implications". *Id. at 426.* Interpreting that standard, the court spoke of actions which are "extraordinary, i.e., one involving 'fundamental business strategy' or 'long term goals.'" *Id. at 427.*

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

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

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

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."

In 2002, the Staff noted "that the presence of ***widespread public debate*** regarding an issue is among the factors to be considered in determining whether proposals concerning that issue 'transcend the day-to-day business matters.'"

Finally, 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."*** 1998 Interpretive Release (emphasis added).

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

Turning to the subject matter of the proposal, the fact that censorship and surveillance by ISPs is a significant policy issue is perhaps best shown through the Company's own assertion that it is a significant policy issue.

On August 13, 2008 AT&T's Senior Vice-President – Public Policy and Chief Privacy Officer, Dorothy Attwood, wrote a letter to Congress in response to inquiries about the use of deep packet inspection (an Internet filtering technology that enables data mining, eavesdropping, and censorship). In that letter Ms. Attwood, stated that Congress was right to be concerned because these capabilities posed ***"significant policy questions"***. Exhibit B (emphasis added).

Just over a month later on September 25, 2008, in Ms. Attwood's testimony to Congress (cited in the Company's no-action request at Company Annex C) on the same issue, she stated ***"Your interest in these matters surely is warranted."*** (emphasis added). She went on to state that these kinds of technologies "that involve tracking consumer web browsing and search activities, ***raise important consumer-privacy concerns that policymakers and industry must carefully weigh.***" (emphasis added).

If the issue of ISP network management technologies and practices is an important enough issue for policymakers to consider, is that not evidence enough that it is a "significant policy issue" that warrants shareholder attention? See *Yahoo!* (April 13, 2007) (permissible proposal focusing on Internet privacy, proponent demonstrated significant policy issue by documenting Congressional interest in the issue).

But these quotes are only the beginning of a substantial body of evidence that there is widespread public interest in censorship and public expectations of privacy on the Internet, in general, and with ISPs specifically.

Consider the enormous amount of mainstream media and business press coverage of the issue of surveillance, network management and censorship over the last six months (Exhibit C):

BusinessWeek
AT&T to Get Tough on Piracy, November 7, 2007
Congress to Push Web Privacy, August 14, 2008
The Candidates are Monitoring your Mouse, August 28, 2008

CNN
Tracking Of Users Across Web Sites Could Face Strict Rules , July 14, 2008
Free speech is thorny online, December 17, 2008

Christian Science Monitor
YouTube to McCain: No DMCA pass for you, October 15, 2008

Financial Times
Google founders in web privacy warning, May 19, 2008
FCC signals its authority over web access, July 29, 2008

Los Angeles Times
Technology stokes new Web privacy fears , July 14, 2008
FCC slams Comcast for blocking Internet traffic, vows to police ISPs , August 1, 2008

MSNBC
ISPs pressed to become child porn cops, October 16, 2008
The trouble with 'deep packet inspection', October 16, 2008

National Public Radio

FCC Rules Against Comcast, August 4, 2008
Google violates its 'don't be evil' motto , November 18, 2008

New York Times

Ad-Targeting Companies and Critics Prepare for Senate Scrutiny, July 8, 2008
An Imminent Victory for 'Net Neutrality' Advocates, July 11, 2008
F.C.C. Vote Sets Precedent on Unfettered Web Usage, August, 2, 2008
Applications Spur Carriers to Relax Grip on Cellphones, August 4, 2008
Web Privacy on the Radar in Congress, August 11, 2008
AT&T Mulls Watching You Surf, August 14, 2008
Comcast Says No New Traffic Management Plan Yet, August 21, 2008
McCain Fights for the Right to Remix on YouTube, October 14, 2008
Banks Mine Data and Pitch to Troubled Borrowers, October 22, 2008
Big Tech Companies Back Global Plan to Shield Online Speech, October 28, 2008
Does AT&T's Newfound Interest in Privacy Hurt Google?, November 20, 2008
Campaigns in a Web 2.0 World, November 3, 2008
How Obama Tapped Into Social Network Power, November 9, 2008
You're leaving a digital trail – do you care?, November 29, 2008
Google's Gatekeepers , November 30, 2008
Proposed Web Filter Criticized in Australia , December 12, 2008
Yahoo Limits Retention of Search Data, December 18, 2008

Jim Leher News Hour

FCC Rules Comcast Violated Internet Access Policy, August 1, 2008

Philadelphia Inquirer

Comcast agrees to sign New York's anti-porn code , July 21, 2008
FCC orders Comcast to change Internet practices, August 1, 2008

Saint Louise Post-Dispatch

FCC rules against Comcast for blocking Internet traffic, August 1, 2008

San Francisco Chronicle

FCC ready to take on ISP limits, July 29, 2008
Tarnished tech firms to adopt code of conduct, October 25, 2008
Group hopes to shape nation's privacy policy , November 17, 2008 (group sponsored by AT&T)

Washington Post

FCC Chairman Seeks to End Comcast's Delay of File Sharing , July 12, 2008
Lawmakers Probe Web Tracking, July 17, 2008
Who Should Solve This Internet Crisis? , July 28, 2008
Lawmakers Seek Data On Targeted Online Ads , August 5, 2008
Some Web Firms Say They Track Behavior Without Explicit Consent , August 12, 2008
Telecom Reporting Rule May Be Eased, September 5, 2008
Politics and Social Networks: Voters Make the Connection, November 3, 2008
Under Obama, Web Would Be the Way Unprecedented Online Outreach Expected, November 10, 2008
A New Voice in Online Privacy, November 17, 2008 (group sponsored by

AT&T)
Verizon Staff Viewed Obama's Account, November 21, 2008
Wikipedia Censorship Sparks Free Speech Debate, December 9, 2008
RIAA's New Piracy Plan Poses a New Set of Problems, December 19, 2008

Wall Street Journal
Cuomo's Probe Spurs Internet Providers to Target Child Porn , June 11, 2008
Limits on Web Tracking Sought , July 15, 2008
Charter Delays Plan for Targeted Web Ads, June 25, 2008
FCC to Rule Comcast Can't Block Web Videos, July 28, 2008
Editorial on net neutrality., July 30, 2008
Google, Yahoo, Microsoft Set Common Voice Abroad, October 28, 2008 (GNI – see discussion below)
Google Wants Its Own Fast Track on the Web, December 15, 2008 (citing pivotal role of AT&T)
Music Industry to Abandon Mass Suits, December 19, 2008 (citing pivotal role of ISPs)

News database searches for terms such as "ISP privacy"; "ISP censorship"; "ISP freedom of speech"; and "ISP surveillance" for 2008 result in over 1,000 additional stories.

As one can see, a fair number of these issues involve the Federal Communications Commission ("FCC") investigation of Comcast's network management practices. The Comcast case originated in October 2007, when the Associated Press reported that its own tests indicated Comcast "actively interferes" with attempts by some high-speed Internet subscribers to share files on peer-to-peer networks. Comcast's interference apparently was both surreptitious and disguised to prevent user detection. FCC Chairman Kevin Martin described the situation this way.

> Would anyone here actually be OK if the Post Office was opening your mail and deciding that they didn't want to bother delivering it and hiding that fact by sending it back to you stamped 'address unknown, return to sender'? Or would anyone here be OK if someone sent them a First Class letter, and the Post Office decided that they would open it, and deciding that because the mail truck was full sometimes, they would make the determination that your letter could wait, and then they would hide that fact from you, the fact that they had read your letter and opened it, and that they decided to delay it? Unfortunately, this was exactly the practice that Comcast was engaging in with their own subscribers' Internet traffic,

The Company is sure to argue that this has nothing to do with its policies and practices, because the FCC case was focused on Comcast and AT&T does not engage in such activities. But that misses the question asked by the ordinary business rule. The FCC Comcast case, and the issues that Chairman Martin describe, demonstrate that ISP network management issues are significant policy issues that are widely debated in the executive and legislative branches of government.

The significance of this as a policy issue is also highlighted by recent polling data from the Consumers Union, the nation's largest consumer group, which shows the following:

> 72% are concerned that their online behaviors were being tracked and profiled by companies

54% are uncomfortable with third parties collecting information about their online behavior

93% of Americans think Internet companies should always ask for permission before using personal information

http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

Perhaps that is why AT&T has taken a central role in sponsoring and helping to establish a new Washington, D.C.-based policy organization called the Future of Privacy Forum (www.futureofprivacy.org), whose mission statement flatly asserts the following:

> Society is approaching a turning point that could well determine the future of privacy. Policy-makers and business leaders soon will make decisions about technology practices that will either ensure that data is used for the benefit of individuals and society, or take us down a path where we are controlled by how others use our data.

With such language coming from the business sector – from AT&T - it cannot be an overstatement to say that a significant social policy issue is at stake here. In fact, it is impossible to reconcile the arguments of AT&T's counsel in its no-action request with these factual assertions made by the Company and an organization it has been instrumental in establishing. Public expectations of privacy is clearly a significant policy issue – and the Company knows it.

A number of other significant events have occurred over the last year which illustrate this point. In May 2008 Charter Communications announced that it was testing a new "service" for its high-speed Internet customers which would permit the company to deduce customers' desires and provide them with highly-targeted ads. The service relies on technology called deep packet inspection (DPI), in which hardware scans the actual content of traffic flowing across the ISP's network, to track the surfing habits of subscribers.

The terms of the program triggered concern from several quarters, including Congress. House Telecommunications Subcommittee, members Edward Markey (D-MA) and Joe Barton (R-TX) sent a letter to Charter's president, asking that the program be stopped until it could be evaluated by Congress. The concern has been that DPI may violate multiple privacy laws and makes it even easier for an ISP to block sites or actively degrade services.

Charter subsequently announced a suspension of its DPI program. But similar initiatives are likely, from Charter and others. The Wall Street Journal noted: "Because cable operators often provide customers with both Internet and TV service, the potential to use intelligence about customers across different platforms -- by, for example, targeting television ads based on Web-surfing behavior -- has enormous potential, analysts say. But it also sets off some alarm bells. 'It requires crossing a whole series of Rubicons regarding customer privacy,' says Craig Moffett, an analyst at Sanford C. Bernstein. ... Given the importance of the new revenue stream to cable operators, Charter's cold feet are likely to send operators looking for some new approaches -- but not back off entirely. 'They are going to do this, so it's a matter of when and not if,' said Moffet."

Accordingly, on September 25, 2008 the Unites States Senate Committee on Commerce, Science and Transportation held a hearing entitled "Hearing on Broadband Providers and Consumer Privacy." It was at that hearing that the Company, through Ms. Attwood, stated ***"Your interest in these matters surely is warranted."*** (emphasis added).

With regard to censorship concerns, consider the censorship incident involving Verizon in September 2007, when Verizon Wireless denied a request by Naral Pro-Choice America, the abortion rights group, to use the company's network for a text-messaging program for individuals who had agreed to receive the messages. Verizon said the subject of the text messages was too "controversial." Following a New York Times story on the incident, Verizon permitted the campaign, saying its earlier decision had been based on "an incorrect interpretation of a dusty internal policy.'" Verizon continues to assert its right to decide what text messages are permissible but has yet to disclose on what grounds such decisions will be made.

Finally, in December, AT&T and a number of other ISPs reportedly agreed to adopt a "three-strikes" program under which customers who have been suspected of pirating copyrighted material on three occasions would be cut off from the Internet. See The Wall Street Journal, *Music Industry to Abandon Mass Suits*, December 19, 2008 (citing pivotal role of ISPs) and The Washington Post, *RIAA's New Piracy Plan Poses a New Set of Problems*, December 19, 2008. While there is no argument that piracy is wrong, the European Commission recently struck down a similar system referring to such plans as "measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access." With the Internet increasingly becoming a necessity for ensuring full participation in our society, democracy and economy such agreements take on added significance.

All of these examples illustrate the point made by Ms. Attwood, Congress, FCC Chairman Martin, the Consumers Union poll, and media attention – i.e.,the impact of ISP network management on freedom of speech and public expectations of privacy is a significant social policy issue subject to widespread public debate. We respectfully request the Staff concur with this conclusion and find that the Proposal is not excludable under the ordinary business exclusion.

The Proposal is not excludable under cases related to "procedures for protecting customer information"

The Company first argues that the Proposal should be excluded because it focuses on "procedures for protecting customer information." We believe this argument fails for a number of reasons.

First, even assuming that customer privacy policies have been historically an issue excluded from shareholder proposals *per se*, circumstances have changed such that it should no longer be considered excludable. For many years issues such as nuclear power, executive compensation, and employee health care were considered mundane matters that were not appropriate for shareholders to consider. Over time, however, the public and policymakers took a growing interest in these issues such that the Staff changed its position and began to regard the issues as significant policy issues that transcend the day-to-day affairs of the company. As demonstrated above, we believe that for Internet service providers like AT&T, the issues of public expectations of privacy, freedom of expression and network management are no longer mundane matters that are not rightfully subject to shareholder attention.

As the role of the Internet has become more and more pervasive in all aspects of our lives, censorship and privacy expectations are becoming of greater interest to the public. AT&T is a critical gatekeeper of our access to speak and be active on the Internet and in society.

Americans realize that the Company's conduct has a significant impact on the health and vitality of our society and for that reason, we believe we have the right to bring the issue before fellow shareholders for consideration.

But we also believe that there is not a *per se* exclusion of shareholder proposals that address privacy issues. In *Cisco Systems Inc.* (July 13, 2002), the proposal focused on the freedom of expression, association and privacy – specifically requesting a report:

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

Like *Cisco*, the Proposal seeks to address the significant privacy and censorship issues that the Company faces. For a hardware and software company like Cisco, an inquiry into the privacy and censorship implications of its business would logically focus on the capabilities of its hardware and software. For an Internet service provider like AT&T, the inquiry appropriately focuses on the impact of its Internet network management practices. We urge the Staff to conclude that the Proposal is analogous to *Cisco*.[1]

Also consider *Yahoo! Inc.*, (April 13, 2007), in which the shareholder proposal requested that the company's management implement policies that would protect user data and prevent censorship:

> **Therefore, be it resolved,** that shareholders request that management institute policies to help protect freedom of access to the Internet which would include the following minimum standards:
>
> 1) Data that can identify individual users should not be hosted in Internet restricting countries, where political speech can be treated as a crime by the legal system.
>
> 2) The company will not engage in pro-active censorship.
>
> 3) The company will use all legal means to resist demands for censorship. The company will only comply with such demands if required to do so through legally binding procedures.
>
> 4) Users will be clearly informed when the company has acceded to legally binding government requests to filter or otherwise censor content that the user is trying to access.
>
> 5) Users should be informed about the company's data retention practices, and the ways in which their data is shared with third parties.
>
> 6) The company will document all cases where legally-binding censorship requests have been complied with, and that information will be publicly available.

In *Yahoo*, the proponent made two important points in defense of the proposal. First, it pointed out that the *Yahoo* proposal, like our Proposal, "deals with the same core policy issue as the proposal in *Cisco*, except in the context of providing Internet services rather than hardware or software . . . " For the same reason we believe that the Proposal is permissible.

---

1 We also note that a virtually identical proposal has received over 28% of the vote at the last three meetings of Cisco. Clearly a significantly large number of shareholders feel that censorship and privacy issues are critically important.

Second, the *Yahoo* proponents argued that their proposal was not excludable because in Congress and the executive branch serious public policy concerns have been raised. As demonstrated above, there has been a significant amount of attention paid to these issues in Congressional hearings and at the FCC.

These two cases, *Cisco* and *Yahoo!*, demonstrate that privacy and censorship issues are not excludable when they involve significant policy issues and focus on the company's impacts on these societal values.

It is also evident that the Proposal differs significantly from the cases cited by the Company in its no-action letter request.

Verizon Communications Inc. (February 22, 2007). The primary distinguishing feature between the *Verizon* proposal and the AT&T Proposal is that *Verizon* was narrowly focused on the privacy of the company's customers. The current AT&T Proposal in contrast focuses on ***the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy***. The focus of the Proposal is not on customer privacy or privacy policies, but ratheron Internet network management practices and their impact on public expectations of privacy. Perhaps the best way to describe this difference is to analogize the issue to environmental issues. It has long been permissible to focus on eliminating or minimizing the harmful impacts of company activities (even core business activities) on the environment or public health. See Staff Legal Bulletin No. 14C. The AT&T Proposal follows that model by focusing on the harmful impacts of company activities, but in this case, on social "goods" such as public expectations of privacy. Furthermore, the focus is not limited to the narrow subject of customer privacy or privacy policies because the Company's Internet network management practices affect many more people than simply customers. Because of the practice of "peering," AT&T's network is used by a vast array of Internet users as their data and content are transmitted across the Internet. In that way the subject matter of the Proposal reaches a population of people that is much broader than the Company's customers. Finally, the Proposal deals with the issue of freedom of expression such that customer privacy issues become a minority subset of issues that would be addressed within the context of public policy and public expectations of privacy – a focus that is clearly not on the day-to-day mundane affairs of the Company.

Bank of America Corp. (March 7, 2005). That case is different than the Proposal because that proposal requested a rote cataloging of existing procedures for ensuring confidentiality. In effect it was simply a policy disclosure request. This Proposal, in contrast, goes beyond such a day-to-day issue, and requests a discussion of the social policy issues. In fact the Proposal is not even focused on privacy policies, but rather the impact of network management practices on public expectations of privacy. Furthermore, in that case 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 and its value as a precedent is severely limited. Finally, the *Bank of America* case did not address privacy in the context of the Internet. Public expectations of privacy on the Internet are the subject of widespread public debate, unlike privacy related to banking transactions.

Applied Digital Solutions, Inc. (March 25, 2006). In that case the proposal was excluded because it related to "product development". Consequently, *Applied Digital Solutions, Inc.* is not relevant to this discussion and cannot be a basis for exclusion.

Citicorp (January 8, 1997). That proposal was excluded for "monitoring illegal transfers through customer accounts." Specifically, that proposal sought a review of existing monitoring policies with respect to an obscure and highly detailed issue; the proponent did very little to document how it constituted a significant social policy issue. As such, *Citicorp* is not applicable.

In summary, it is critical to place this Proposal in its proper context. The Internet network management practices of have real world impacts on freedom of expression and public expectations of privacy. Those impacts and company practices have come under the scrutiny of regulators, Congress and the public. Our society is currently engaged in a debate about these issues. As such, the cases cited by the Company cannot be the basis for excluding the Proposal. Those cases address the minutia of customer privacy policies, not the negative impacts, real and potential, of AT&T's Internet management activities on fundamental societal values such as privacy and free speech. For those reasons we respectfully request the Staff conclude the Company has not met its burden of persuasion and to reject the Company's argument.

The Company's discussion of "public policy overlap" is not an accurate description of Rule 14a-8

Almost as an aside, the Company argues that even if the Proposal has some "overlap" with public policy, it is still excludable. This argument turns the ordinary business rule on its head. *Roosevelt v. E.I. DuPont de Nemours & Company*, 958 F. 2d 416 (DC Cir. 1992) and *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877 (S.D.N.Y. 1993) make it abundantly clear that "the proposal may be excluded only after the proposal is also found to raise no substantial policy consideration." Id at 891. Thus, to argue that the proposal can be excluded regardless of whether or not it touches upon a significant social policy issue is directly contrary to the rule.

Second, as was discussed at length earlier, it is clear that AT&T is currently facing a significant social policy issue. To imply that the Proposal merely overlaps with a significant policy issue is misplaced and cannot provide sufficient reasons to overcome the Company's significant burden of persuasion to exclude the Proposal.

Finally, the Company's reliance on *Microsoft* (September 29, 2006); *Pfizer Inc.* (January 24, 2006); and *Marathon Oil* (January 23, 2006) are completely misplaced because those proposals evidently did not implicate any significant social policy issues. With respect to *Microsoft*, that proposal, similar to *Bank of America Corp.* (February 21, 2006), was focused exclusively on *financial issues* and did not address large social policy issues like public expectations of privacy and freedom of expression. Similarly, the *Pfizer* and *Marathon Oil* proposals were focused on "the ***economic*** effects of the HIV/AIDS, Tuberculosis and Malaria pandemics on our Company's ***business*** strategy." (emphasis added). Those two proposals were excluded as implicating an "evaluation of risk" - a unique circumstance that was addressed in Staff Legal Bulletin 14C. The Company has not made any evaluation of risk argument and therefore the proposals in those cases are irrelevant. Consequently, to equate these three proposals, which were focused solely on company specific financial issues as opposed to significant policy issues that transcend the ordinary business of the company, is to misapprehend the meaning of those cases.

The Proposal does not constitute a request for a legal compliance program

The Company next argues that simply because there may be some legal compliance implication to a proposal it is excludable. This is clearly not the case as illustrated by *Exxon Mobil Corp.* (March 18, 2005) cited favorably by the Staff in Staff Legal Bulletin 14C. That

proposal was a request for a report "on the potential environmental damage that would result from the company drilling for oil and gas in protected areas s such as IUCN Management Categories I-IV and Marine Management Categories I-V, national parks, monuments, and wildlife refuges (such as the Arctic National Wildlife Refuge), and World Heritage Sites". It would be virtually impossible for such a report to be produced without a discussion of compliance with the extensive environmental laws that govern those federally protected areas. Assuming that the Proposal does in fact require some discussion of legal compliance, it is clear from *Exxon Mobil Corp.* that it is permissible.

Reviewing the no-action letters presented by the Company, it is also evident that they do not apply. First, in *Allstate Corporation* (February 16, 1999) the proponents sought to create an entirely new committee that would hire experts in "the fields of: Criminal Law, McCarran Ferguson Act, Bad Faith Insurance Actions, Shareholders Derivative Actions and a Financial Management firm be organized for the purpose of investigating the issues raised". The *Allstate* proposal is distinct in two ways from the Proposal. First, *Allstate* sought to create a whole new compliance structure for the company. The Proposal, in contrast, does not do that – it requests a discussion on social policy issues. Second, the *Allstate* proposal sought a very high level of micro-management that the Proposal does not. That proposal sought to dictate how the compliance program would occur with specifics about certain fields of law and the need to hire specific personnel to staff the committee. The Proposal in contrast is not even impliedly interested in those intricate details and plainly focuses on the significant social policy issues facing the Company.

In *Duke Power Company* (February 16, 1999) the shareholder sought very detailed information on the technical aspects of a highly regulated portion of the company's business. In fact the resolve clause ran almost 300 words and included a list of very specific technical information on particular facilities. It is erroneous to analogize the Proposal to *Duke* for the very simple reason that the *Duke* proposal achieved an extraordinary level of micro-management in a very highly regulated aspect of pollution controls. The Proposal in contrast deals with a high policy level discussion of the impact of network management practices on public expectations of privacy and freedom of expression.

The *Halliburton Company* (March 10, 2006) proposal requested a report "on the policies and procedures adopted and implemented to reduce or eliminate the reoccurrence of such [criminal] violations and investigations." This proposal was excluded as addressing "general conduct of a legal compliance program." What is distinct about *Halliburton* is that the proposal sought a report on existing policies and focused on specific violations of federal law.

But beyond these cases, it is clear from the plain language of the Proposal that it does not focus on the Company's legal compliance program. It focuses on the Company's impact on society, and to the extent that a discussion of legal compliance would be necessary, we would observe that virtually any significant social policy issue has legal compliance implications in some form. To conclude, as AT&T would have, that the presence of a legal compliance issue is fatal would make the exception consume the rule. In sum, the Proposal does not seek to interfere in the day-to-day business of legal compliance programs and as a consequence does not qualify for the ordinary business exclusion.

The Proposal does not seek to direct the Company's lobbying efforts

The Company also argues that the Proposal inappropriately involves the Company in the

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

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

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

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

Furthermore, note that the previously discussed *Yahoo! Inc.*, (April 13, 2007) specifically demonstrated that it focused on a significant social policy issue by citing a specific piece of legislation that addressed similar issues.

As John W. White, then the Director of the Division of Corporation Finance pointed out to the American Bar Association in 2008, the issue is whether the proposal asks the company to directly lobby on a specific issue (http://ww.sec.gov/news/speech/2008/spch08il08iww.html) . Clearly, this Proposal does not ask the Company to directly lobby Congress on any issue. The Proposal seeks an examination of the public policy issues and does not seek any lobbying or for that matter

seek the implementation of any policies or procedures.

Finally, the Company cites a number of proposals on the issue of net neutrality. Those proposals, *Microsoft Corporation* (September 29, 2006) and *Yahoo!* (April 5, 2007), were excluded on the very narrow grounds that they sought an evaluation of the impact of expanded government regulation of the Internet. The proposals sought a report "on the Company's rationales for supporting and/or advocating public policy measures that would increase government regulation of the Internet" and focused on company lobbying activities. The proposals took particular exception to a letter sent by the companies to a congressional committee. Clearly these proposals are categorically different than the Proposal in that they focused on Company lobbying efforts.

As such, we respectfully ask the Staff to reject the Company's arguments and conclude that it must include the Proposal in its proxy materials.

Significant policy issue conclusion

In the preceding sections we have fully refuted the Company's arguments concerning customer information, compliance programs, and lobbying exclusions. It is clear than none of these exclusions apply to the Proposal. But more importantly it is clear that the impact of the company's network management practices on public expectations of privacy and freedom of expression are a significant public policy issue confronting the company – and under Rule 14a-8, that is the fundamental question.

We also observe that the Company is not arguing that the Proposal seeks to micro-manage the Company's activities. To the extent that such an argument is implied in the Company's letter we would point out that the Proposal clearly functions at an appropriately general level. The Proposal expressly seeks an examination of public policy issues and impacts on society, which is a level of discussion appropriate for a shareholder audience. Nothing about the Proposal seeks specific information about the details of Internet network management practices or methods for implementing complex policies. It is focused on the Company examining the ***effects*** of its network management practices on the public goods of freedom of expression and expectations of privacy. While such an examination obviously requires some general discussion of network management practices, it clearly does not require the company to delve into the technical and minute details of the Company's business. Technologies change and the hardware and software that the Company employs to manage its network change, but that is not the subject of this Proposal. It is about how the Company impacts our human rights. That is an issue shareholders readily understand. See *Microsoft Corporation* (September 14, 2000) (phrases like "freedom of association" and "freedom of expression" are not too vague).

As was discussed earlier, these issues are significant policy issues confronting the Company. As shareholders we are concerned that the Company is not addressing these issues, at a strategic level, sufficiently. The Company has become gatekeepers to critical political, social and economic discourse in our country. For the welfare of our Company and our society, the Company must engage in a thoughtful and meaningful examination of these issues.

The Company has not substantially implemented the Proposal

The Company claims that the Proposal's request has been substantially implemented

through its privacy policies and through two public statements. However, based on a review of the website and the applicable no-action letters issued by the Staff it is clear that the Company has not met the Rule 14a-8(i)(10) standard because the privacy policies and statements:

- do not address freedom of speech and censorship issues;
- do not address the Company's role as a content provider;
- are conclusory and therefore do not contain an examination of the issues by the Board; and
- are not presented in a single document for a shareholder audience.

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

The policies and statements provided clearly do not address censorship or freedom of speech issues. As the Pearl Jam incident illustrates, AT&T is a content provider. However, the material provided by the Company fails to address the Company's proactive role in interfering with the flow of information as exemplified in the Pearl Jam episode. For that reason, a substantial portion of the Proposal has gone unaddressed.

The policies and statements also do not address the issue of Internet users who are not AT&T customers. Due to the essential practice of "peering,"AT&T carries data and content for a vast number of Internet users that have absolutely no customer relationship with AT&T.

In addition, we have requested an *examination* of these issues and that implicitly calls for a presentation of differing ideas and approaches. It could mean discussing what other companies have done in the past or are proposing to do. The Proposal does not ask for a specific result or policy, but an exploration of the issues in the context of the significant policy concerns that have been expressed as they apply to the Company's future as a profitable and socially responsible company. Clearly AT&T's privacy policy and the public statements do not do that.

Furthermore, the privacy policy is intended to communicate information to *customers* and the public statements were intended for legislators and regulators, while the Proposal requests information for *shareholders*. This is not a minor distinction. The concerns of shareholders can be very different than the concerns of its customers, legislators or regulators.

Next, the websites do not present the information in the same form as we request. The Proposal asks for a single report. While the Company cites to the privacy policy and public statement, we observe that there are other privacy policies under the umbrella of AT&T. For example, there is a separate and distinct privacy policy at http://www.wireless.att.com/privacy/, http://helpme.att.net/article.php?item=8620 (AT&T Internet Service and Video Services policy), and http://www.att.com/gen/privacy-policy?pid=7911 (AT&T|DISH network service). We are asking the Company to provide shareholders with the Board's discussion in a unified manner, rather than over multiple websites perhaps containing duplicative and conclusory statements. In this regard consider *Newell Rubbermaid Inc.* (February 21, 2001) in which the Staff required inclusion of a proposal requesting that the board prepare a report on the company's "glass ceiling" progress, including a review of specified topics. The company claimed that it had already considered the concerns raised in the proposal and that it had publicly available plans in place. Despite those arguments, it was beyond dispute that the company had not prepared a report on the topic. Similarly,

while the Company may argue that it has indirectly done what we ask, it has not provided documentation in a single report that substantially covers the issues. See also *PPG Industries, Inc.* (January 22, 2001) (proposal deemed not substantially implemented by a variety of policies when proponents argued that the essence of the proposal was to create a single document that explicitly and in one place committed the company to the enumerated principles).

In addition, the policies and statements are not the product of a ***board*** examination. On a number of occasions the Staff has concurred that when a proposal is focused on board level action, it is not sufficient for the company to argue that employees and management are addressing the issue. For example, in *NYNEX Corporation* (February 16, 1994), the permitted proposal requested the company establish a four-member committee of its board of directors to evaluate the impact of various health care proposals on the company. The company unsuccessfully argued that it had substantially implemented the proposal because it had already established a Committee on Benefits, which oversaw the administration and effectiveness of all of the NYNEX employee benefits plans and programs, including the medical programs. In addition, the company argued that it was working to explore solutions to the specific issue of health care cost containment through its collaboration with unions, research institutes and business groups. In the case now before the Staff, the Company has not even argued that the Board is addressing these issues. Rather, as in *NYNEX*, the Company has argued that it is taking other steps, at the employee/management level, to address the issue, but not the essential step of addressing this issue at the board level. As the proponent in *NYNEX* rightfully pointed out, employee or management activities are no substitute for steps taken by board members and consequently the Proposal has not been substantially implemented. We respectfully request the Staff agree that employee/management level activities are not a substitute. See also, *NYNEX Corporation* (February 18, 1994) (creation of a "Facilities Closure and Relocation of Work Committee" composed of four outside directors, two employee representatives and two representatives of affected committees).

Similarly, in *Associates First Capital Corporation* (March 13, 2000), the permitted proposal requested the company establish a committee of directors to develop and enforce policies to ensure that "employees do not engage in predatory lending practices." In that case, the company argued, unsuccessfully, that comprehensive internal procedures developed and implemented at the managerial level had substantially implemented the proposal. The proponent successfully pointed out that the proposal did not request management action, but instead focused on a board level review of the issue, and that consequently the proposal had not been substantially implemented. Consequently, the Company has not substantially implemented the Proposal. See also, *Conseco, Inc.* (April 15, 2001) (same).

Finally, while AT&T is correct to cite many cases for the conclusion that companies are required to "substantially implement" proposals rather than "fully implement" proposals, what is critical is that it must, at the very least, address the core concerns raised by the proposal. See *Dow Chemical Company* (February 23, 2005); *ExxonMobil* (March 24, 2003); *Johnson & Johnson* (February 25, 2003); *ExxonMobil* (March 27, 2002); and *Raytheon* (February 26, 2001). In all of these cases the Staff rejected company arguments and concluded that the company's disclosures were insufficient to meet the substantially implemented standard. The case of *Wendy's International* (February 21, 2006) provides a particularly comparable example of the Staff rejecting a company's argument that information provided on a website was sufficient. In *Wendy's* the company argued that it had provided the requested sustainability report on its website and that the information contained on the website was sufficient. The proponent successfully demonstrated that the website contained no documentation that the company engaged in a discussion of the

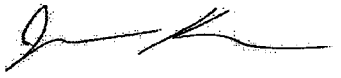
issues, as requested, and that the website only contained "vague statements of policy." Similarly, the company has not demonstrated that it has engaged in the board examination requested and the information provided does not address the core issue of censorship and freedom of speech raised in the Proposal. Consequently, we respectfully request that the Staff not concur with the Company and not permit it to exclude the Proposal on Rule 14a-8(i)(10) grounds.

Conclusion

In conclusion, we respectfully request the Staff to inform the Company that Rule 14a-8 requires a denial of the Company's no-action request. As demonstrated above, the Proposal is not excludable under any of the criteria of Rule 14a-8. Not only does the Proposal raise a critical social policy issue facing the nation and the Company, but it raises that issue in a manner that is appropriate for shareholder consideration. In the event that the Staff should decide to concur with the Company and issue a no-action letter, we respectfully request the opportunity to speak with the Staff in advance.

Please contact me at (971) 222-3366 or jkron@trilliuminvest.com with any questions in connection with this matter, or if the Staff wishes any further information. Also, pursuant to Staff Legal Bulletin Nos. 14B and 14D we request the Staff fax a copy of its response to (928) 222-3362 and/or email a copy of its response to jkron@trilliuminvest.com

Sincerely,



Jonas Kron,
Senior Social Research Analyst

Enclosures

cc:

David B. Harms
Sullivan & Cromwell LLP

Alexander Rakosi
Sullivan & Cromwell LLP

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

Dawn Wolfe
Social Research & Advocacy Analyst
Boston Common Asset Management, LLC

Aditi Vora,
Social Research Analyst
Calvert Asset Management Company, Inc.

FTC Staff Report:

Self-Regulatory Principles For Online Behavioral Advertising

February 2009

TABLE OF CONTENTS

FTC STAFF REPORT:
SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING

EXECUTIVE SUMMARY

Since the emergence of "e-commerce" in the mid-1990s, the online marketplace has continued to expand and evolve, creating new business models that allow greater interactivity between consumers and online companies. This expanding marketplace has provided many benefits to consumers, including free access to rich sources of information and the convenience of shopping for goods and services from home. At the same time, the ease with which companies can collect and combine information from consumers online has raised questions and concerns about consumer privacy.

Starting in 1995, the Federal Trade Commission ("FTC" or "Commission") has sought to understand the online marketplace and the privacy issues it raises for consumers. The Commission has hosted numerous public workshops and has issued public reports focusing on online data collection practices, industry self-regulatory efforts, and technological developments affecting consumer privacy. As part of this effort, the Commission has examined online behavioral advertising – the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests. In November 2007, the FTC held a two-day "Town Hall," which brought together numerous interested parties to discuss online behavioral advertising in a public forum.

Participants at the Town Hall discussed the potential benefits of the practice to consumers, including the free online content that online advertising generally supports, the personalized advertising that many consumers may value, and a potential reduction in unwanted advertising. They also discussed the privacy concerns that the practice raises, including the

invisibility of the data collection to consumers; the shortcomings of current disclosures about the practice; the potential to develop and store detailed profiles about consumers; and the risk that data collected for behavioral advertising – including sensitive data regarding health, finances, or children – could fall into the wrong hands or be used for unanticipated purposes. Following the Town Hall, FTC staff released for public comment a set of proposed principles (the "Principles") designed to serve as the basis for industry self-regulatory efforts to address privacy concerns in this area.

In drafting the Principles, FTC staff drew upon its ongoing examination of behavioral advertising, as well as the public discussion at the Town Hall. Staff also attempted to balance the potential benefits of behavioral advertising against the privacy concerns. Specifically, the Principles provide for transparency and consumer control and reasonable security for consumer data. They also call for companies to obtain affirmative express consent from consumers before they use data in a manner that is materially different than promised at the time of collection and before they collect and use "sensitive" consumer data for behavioral advertising. In addition to proposing the Principles, staff also requested information concerning the use of tracking data for purposes unrelated to behavioral advertising.

Staff received sixty-three comments on the Principles from eighty-seven stakeholders, including individual companies, business groups, academics, consumer and privacy advocates, and individual consumers. Many commenters addressed the Principles' scope, an issue that cuts across each of the individual principles. In particular, commenters discussed whether the Principles should apply to practices involving information that is not personally identifiable and whether they should apply to "first party" and "contextual" behavioral advertising models. As discussed further in this Report, staff believes that the Principles should apply to data that could

reasonably be associated with a particular consumer or computer or other device, regardless of whether the data is "personally identifiable" in the traditional sense. Indeed, in the context of online behavioral advertising, rapidly changing technologies and other factors have made the line between personally identifiable and non-personally identifiable information increasingly unclear. Moreover, this approach is consistent with existing self-regulatory efforts in this area.

Staff agrees with some of the commenters, however, that the Principles' scope could be more narrowly focused in two important respects. First, it appears that "first party" behavioral advertising – behavioral advertising by and at a single website – is more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than other forms of behavioral advertising. Second, staff believes that contextual advertising – advertising based on a consumer's current visit to a single web page or a single search query that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result – is likely to be less invasive than other forms of behavioral advertising. Accordingly, staff believes that the Principles need not cover these practices. Staff notes, however, that some of the Principles are based on existing Commission law and policy. Therefore, regardless of the scope of the Principles, companies must still comply with existing legal obligations to provide reasonable security for consumer data. Further, companies must adhere to the promises they make regarding how they collect, use, store, and disclose data, and cannot make unilateral, "material changes" to such promises without consumers' consent.

In addition to addressing the Principles' overall scope, numerous commenters discussed the individual principles. In particular, commenters discussed whether and how to provide transparency and consumer choice for online behavioral advertising. They also raised issues related to the material change principle and questioned how to define "sensitive" data and the

appropriate protections for such data. Relatively few of the commenters answered staff's request for additional information on other uses for tracking data. This Report discusses the main points addressed in the comments, provides further guidance regarding the scope and application of the Principles, and sets forth revised Principles. It also discusses recent initiatives by industry, consumer groups, and others to address the consumer privacy concerns raised by online behavioral advertising.

This Report constitutes the next step in an ongoing process to examine behavioral advertising that involves the FTC, industry, consumer and privacy organizations, and individual consumers. Although the comments have helped to frame the policy issues and inform public understanding of online behavioral advertising, the practices continue to evolve and significant work remains. Some companies and industry groups have begun to develop new privacy policies and self-regulatory approaches, but more needs to be done to educate consumers about online behavioral advertising and provide effective protections for consumers' privacy. Staff, therefore, will continue to examine this marketplace and take actions to protect consumers as appropriate.

I. INTRODUCTION

On December 20, 2007, Federal Trade Commission ("FTC" or "Commission") staff released for public comment a set of proposed self-regulatory principles related to online behavioral advertising – the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests.[1] Staff developed these principles (the "Principles") based on an ongoing examination of the consumer issues raised by behavioral advertising and the public discussion of these issues at the FTC's November 2007 "Ehavioral Advertising" Town Hall.[2] Staff's goals in releasing the Principles were to spur continuing public dialogue about the issues and to encourage industry to develop meaningful self-regulation in this area.

In developing the proposed Principles, staff attempted to balance the privacy concerns raised by online behavioral advertising against the potential benefits of the practice. Consumers have genuine and legitimate concerns about how their data is collected, stored, and used online. They may also benefit, however, from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value. Thus, any self-regulatory program in this area should address practices that raise genuine privacy concerns without interfering with practices – or stifling innovation – where privacy concerns are minimal.

In response to the proposed Principles, staff received over sixty comments from various stakeholders, including industry, privacy advocates, technologists, consumers, academics, and state and foreign governmental entities. The comments have helped to further staff's

---

[1] FTC Staff, *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles* (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

[2] FTC Town Hall, *Ehavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1-2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

understanding of the complex and rapidly evolving online behavioral advertising marketplace. At the same time, the comments raised additional issues and questions for consideration, and many of them called upon Commission staff to provide more guidance. This Report summarizes and responds to the main issues raised in the comments. In addition, the Report provides guidance on the Principles and sets forth revised principles consistent with this guidance.

II. BACKGROUND

A. What Is Online Behavioral Advertising?

Online behavioral advertising involves the tracking of consumers' online activities in order to deliver tailored advertising. The practice, which is typically invisible to consumers, allows businesses to align their ads more closely to the inferred interests of their audience. In many cases, the information collected is not personally identifiable in the traditional sense – that is, the information does not include the consumer's name, physical address, or similar identifier that could be used to identify the consumer in the offline world. Instead, businesses generally use "cookies"[3] to track consumers' activities and associate those activities with a particular computer or device.[4] Many of the companies engaged in behavioral advertising are so-called

---

[3] A cookie is a small text file that a website's server places on a computer's web browser. The cookie transmits information back to the website's server about the browsing activities of the computer user on the site. This includes information such as pages and content viewed, the time and duration of visits, search queries entered into search engines, and whether a computer user clicked on an advertisement. Cookies also can be used to maintain data related to a particular individual, including passwords or items in an online shopping cart. In some contexts, such as where a number of separate websites participate in a network, cookies can be used to track a computer user across different sites. In addition to cookies, there are other devices for tracking online activities, including "web bugs," "web beacons," and "Flash cookies."

[4] As discussed below, however, it may be possible to link or merge the collected information with personally identifiable information – for example, name, address, and other information provided by a consumer when the consumer registers at a website.

"network advertisers," companies that select and deliver advertisements across the Internet at websites that participate in their networks.[5]

An example of how behavioral advertising might work is as follows: a consumer visits a travel website and searches for airline flights to New York City. The consumer does not purchase any tickets, but later visits the website of a local newspaper to read about the Washington Nationals baseball team. While on the newspaper's website, the consumer receives an advertisement from an airline featuring flights from Washington D.C. to New York City.

In this simple example, the travel website where the consumer conducted his research might have an arrangement with a network advertiser to provide advertising to its visitors. The network advertiser places on the consumer's computer a cookie, which is tied to non-personally identifiable information such as the web pages the consumer has visited, the advertisements that the consumer has been shown, and how frequently each advertisement has been shown. Because the newspaper's website is also part of the advertising network, when the consumer visits the newspaper website the network advertiser's cookie identifies the consumer as a visitor to the travel website who likely has an interest in traveling to New York. It then serves the corresponding advertisement for airline flights to New York.

In a slightly more sophisticated example, the information about the consumer's activities on the travel website could be combined with information about the content that the consumer viewed on the newspaper's website. The advertisement served could then be tailored to the consumer's interest in, not just New York City, but also baseball (*e.g.*, an advertisement

---

[5] Ads from network advertisers are usually delivered based upon data collected about a given consumer as he or she travels across the different websites in the advertising network. An individual network may include hundreds or thousands of different, unrelated websites and an individual website may belong to multiple networks.

referring to the New York Yankees).

B. The FTC's Examination of Online Behavioral Advertising

The Federal Trade Commission's involvement with online privacy issues, including behavioral advertising, dates back to the emergence of "e-commerce."[6] Since that time, the Commission has sought to understand the marketplace, to evaluate the costs and benefits of various practices affecting consumers, and to stop unfair or deceptive practices. At the same time, given the dynamic nature of this marketplace and the technologies that make it possible, the Commission has consistently sought to avoid stifling innovation so that responsible business practices could develop and flourish. The Commission has engaged in a continuous dialogue with members of industry, consumer and privacy advocates, technology experts, consumers, and other interested parties. Starting in 1995, the Commission has conducted a series of public workshops and has issued reports focusing on online data collection practices, industry's self-regulatory efforts, and technological efforts to enhance consumer privacy.[7] In addition to these

---

[6] *See, e.g.*, FTC Report, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 3-6 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. This report described the Commission's involvement in online privacy issues and recommended that Congress enact online privacy legislation based upon "fair information practice" principles for consumer-oriented commercial websites.

[7] *See, e.g.*, FTC Town Hall, *Beyond Voice: Mapping the Mobile Marketplace* (May 6-7, 2008), *available at* http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml; FTC Workshop, *Protecting Personal Information: Best Practices for Business* (Apr. 15, 2008, Aug. 13, 2008, and Nov. 13, 2008), *available at* http://www.ftc.gov/bcp/workshops/infosecurity/index.shtml; FTC Workshop, *Security in Numbers: SSNs and ID Theft* (Dec. 10-11, 2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/index.shtml; FTC Staff Report, *Spam Summit: The Next Generation of Threats and Solutions* (Nov. 2007), *available at* http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf; FTC Summit, *Spam Summit: The Next Generation of Threats and Solutions* (July 11-12, 2007), *available at* http://www.ftc.gov/bcp/workshops/spamsummit/index.shtml; FTC Staff Report, *Radio*

policy initiatives, the Commission and its staff have conducted investigations and brought law enforcement actions challenging such practices as deceptive privacy claims and improper disclosure of consumer data.[8]

Frequency IDentification: Applications and Implications for Consumers (Mar. 2005), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf; FTC Workshop, *Radio Frequency IDentification: Applications and Implications for Consumers* (June 21, 2004), *available at* http://www.ftc.gov/bcp/workshops/rfid/index.shtm; FTC Workshop, *Monitoring Software on Your PC: Spyware, Adware and Other Software* (Apr. 19, 2004), *available at* http://www.ftc.gov/bcp/workshops/spyware/index.shtm; FTC Forum, *Spam Forum* (Apr. 30-May 2, 2003), *available at* http://www.ftc.gov/bcp/workshops/spam/index.shtml; FTC Workshop, *Consumer Information Security Workshop* (May 20-21, 2002), *available at* http://www.ftc.gov/bcp/workshops/security/index.shtm; FTC Report, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (Feb. 2002), *available at* http://www.ftc.gov/bcp/reports/wirelesssummary.pdf; FTC Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues* (Dec. 11-12, 2000), *available at* http://www.ftc.gov/bcp/workshops/wireless/index.shtml; FTC Report, *Consumer Protection in the Global Electronic Marketplace: Looking Ahead* (Sept. 2000), *available at* http://www.ftc.gov/bcp/icpw/lookingahead/electronicmkpl.pdf; FTC Workshop, *U.S. Perspectives on Consumer Protection in the Global Electronic Marketplace* (June 1999), *available at* http://www.ftc.gov/bcp/icpw/lookingahead/global.shtm; FTC Staff Report, *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996), *available at* http://www.ftc.gov/reports/privacy/privacy.pdf; FTC Workshop, *Consumer Privacy on the Global Information Infrastructure* (June 1996), *available at* http://www.ftc.gov/bcp/privacy/wkshp96/privacy.shtm.

[8] Since 2001, the Commission has brought twenty-three actions against companies that allegedly failed to provide reasonable protections for sensitive consumer information in both online and offline settings. *See FTC v. Navone*, No. 2:08-CV-01842 (D. Nev. filed Dec. 30, 2008); *United States v. ValueClick, Inc.*, No. 2:08-CV-01711 (C.D. Cal. Mar. 13, 2008); *United States v. American United Mortgage*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006); *In the Matter of Genica Corp.*, FTC Matter No. 082-3133 (Feb. 5, 2009) (proposed consent agreement); *In the Matter of Premier Capital Lending, Inc.*, FTC Docket No. C-4241 (Dec. 10, 2008); *In the Matter of The TJX Cos.*, FTC Docket No. C-4227 (July 29, 2008); *In the Matter of Reed Elsevier Inc.*, FTC Docket No. C-4226 (July 29, 2008); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008); *In the Matter of Goal Fin., LLC*, FTC Docket No. C-4216 (Apr. 9, 2008); *In the Matter of Guidance Software, Inc.*, FTC Docket No. C-4187 (Mar. 30, 2007); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. C-4168 (Sept. 5, 2006); *In the Matter of Nations Title Agency, Inc.*, FTC Docket No. C-4161 (June 19, 2006); *In the Matter of DSW, Inc.*, FTC

1. Online Profiling Workshop

As a part of these efforts, in November 1999 the FTC and the Department of Commerce jointly sponsored a public workshop to examine the privacy implications of "online profiling" – essentially, an early form of online behavioral advertising.[9] Based upon the workshop, the FTC prepared two reports to Congress. The first, *Online Profiling: A Report to Congress* (June 2000) ("June 2000 Report"), described how online profiling operates and addressed the concerns that many of the workshop participants raised about the collection of detailed consumer data and the practice's lack of transparency.[10] The June 2000 Report also described online profiling's potential benefits to consumers, as well as to businesses. These benefits included delivering more relevant ads to consumers, subsidizing free online content, and allowing businesses to market more precisely and spend their advertising dollars more effectively.

The Commission's second report, *Online Profiling: A Report to Congress Part 2*

Docket No. C-4157 (Mar. 7, 2006); *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005); *In the Matter of BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148 (Sept. 20, 2005); *In the Matter of Nationwide Mortgage Group, Inc.*, FTC Docket No. 9319 (Apr. 12, 2005); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005); *In the Matter of Sunbelt Lending Servs., Inc.*, FTC Docket No. C-4129 (Jan. 3, 2005); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004); *In the Matter of Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002); *In the Matter of Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002).

[9] FTC and Department of Commerce Workshop, *Online Profiling Public Workshop* (Nov. 8, 1999), *available at* http://www.ftc.gov/bcp/workshops/profiling/index.shtm.

[10] June 2000 Report, *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf. The June 2000 Report stated that "[m]any commenters at the Workshop objected to networks' hidden monitoring of consumers and collection of extensive personal data without consumers' knowledge or consent; they also noted that network advertisers offer consumers few, if any, choices about the use and dissemination of their individual information obtained in this manner." *Id.* at 10.

Recommendations (July 2000) ("July 2000 Report"),[11] supplemented the first report by addressing self-regulatory principles developed by the Network Advertising Initiative ("NAI"). NAI, an organization consisting of online network advertisers, had developed these principles ("NAI Principles") in response to concerns raised at the 1999 workshop and submitted them to the FTC and the Department of Commerce for consideration. In the July 2000 Report, the Commission commended the NAI companies' efforts in developing principles that included various protections to govern the collection and use of consumer data online.[12] Nevertheless, while acknowledging that "self-regulation is an important and powerful mechanism for protecting consumers," a majority of the Commission recommended that Congress enact "backstop legislation" to address online profiling.[13]

Ultimately, Congress did not enact legislation to address online profiling. In the meantime, with the "burst" of the dot-com bubble, the number of network advertisers declined dramatically such that by the early 2000s, many had gone out of business.[14]

---

[11] July 2000 Report, *available at* http://www.ftc.gov/os/2000/07/onlineprofiling.pdf.

[12] Issued in 2000, the NAI Principles required network advertisers to notify consumers about profiling activities on host websites and to give consumers the ability to choose not to participate in profiling. The NAI Principles applied to both personally identifiable and non-personally identifiable consumer data. Where a member collected personally identifiable information, it had to provide notice and opt-out choice at the time and place of collection. For non-personally identifiable information, notice could appear in the publisher website's privacy policy with a link to the NAI website, where a consumer could opt out. The NAI Principles also imposed certain restrictions on the merger of personally identifiable information with non-personally identifiable information. As discussed in more detail below, NAI recently released revised principles.

[13] *See* July 2000 Report, *supra* note 11, at 10-11.

[14] *See, e.g.*, George Raine, *Dot-com Ads Make a Comeback*, S.F. CHRON., Apr. 10, 2005, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/04/10/BUG1GC5M4I1.DTL (discussing negative impact of dot-com implosion on online advertising generally).

2. Tech-ade Hearings and the Ehavioral Advertising Town Hall

By the middle of the decade, the online advertising market, including the behavioral advertising market, had regained its footing. Indeed, online advertising spending grew dramatically between 2002 and 2006, with estimated sales rising from $6 billion to over $16.6 billion.[15] These changes in the marketplace, and the growing practice of behavioral advertising, were a featured topic at the FTC's November 2006 "Tech-ade" hearings,[16] which examined the consumer protection challenges anticipated over the next ten years. Participants at the hearings described how technological advances had allowed for greater and more efficient use of online profiling (now called "behavioral" advertising, targeting, or marketing) and brought renewed attention to the practice.[17]

In the months after the Tech-ade hearings, staff launched an effort to learn more about online behavioral advertising. At the same time, several organizations petitioned the Commission to reexamine the privacy issues raised by the practice.[18] Further, the announcement

---

[15] *Id. See also* Ryan Blitstein, *Microsoft, Google, Yahoo in Online Ad War*, SAN JOSE MERCURY NEWS, May 19, 2007.

[16] The complete transcripts of the hearings, entitled *Protecting Consumers in the Next Tech-Ade*, are available at http://www.ftc.gov/bcp/workshops/techade/transcripts.html.

[17] *See* Transcript of Hearing Record at 46-107, *Protecting Consumers in the Next Tech-ade* (Nov. 7, 2006), *available at* http://www.ftc.gov/bcp/workshops/techade/pdfs/transcript_061107.pdf (panel discussion entitled "Marketing and Advertising in the Next Tech-ade").

[18] *See, e.g.*, Letter from Ari Schwartz, Executive Director, and Alissa Cooper, Policy Analyst, Center for Democracy and Technology ("CDT"), to J. Thomas Rosch, Commissioner, FTC (Jan. 19, 2007), *available at* http://www.cdt.org/privacy/20070119rosch-behavioral-letter.pdf; Center for Digital Democracy ("CDD") and U.S. Public Interest Research Group, Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2006), *available at* http://www.democraticmedia.org/files/pdf/FTCadprivacy.pdf.

of the proposed merger between Google, Inc. ("Google") and DoubleClick, Inc. in April 2007 raised concerns about the combination of large databases of consumer information and the potential development of detailed consumer profiles.[19] Commission staff met with dozens of industry representatives, technology experts, consumer and privacy advocates, and academics. These meetings aided staff's understanding of the changes to the industry since the 1999 workshop and allowed staff to identify key questions and issues for further discussion.

In November 2007, the FTC held its "Ehavioral Advertising Town Hall," a two-day public meeting that brought together various interested parties to discuss the privacy issues surrounding online behavioral advertising.[20] Based on the discussion, several core principles emerged. First, as discussed above, online behavioral advertising[21] may provide valuable

---

[19] *See* Letter from Jeffrey Chester, Executive Director, CDD, to Deborah Platt Majoras, Chairman, FTC et al. (Dec. 10, 2007), *available at* http://www.democraticmedia.org/files/FTCletter121007.pdf; Letter from Mindy Bockstein, Executive Director, New York State Consumer Protection Board, to Deborah Platt Majoras, Chairman, FTC, Re: DoubleClick Inc. and Google, Inc. Merger (May 1, 2007), *available at* http://epic.org/privacy/ftc/google/cpb.pdf. The Commission approved the merger on December 20, 2007, at the same time that it issued the Principles. *See Statement of Federal Trade Commission Concerning Google/DoubleClick*, FTC File No. 071-0170 (Dec. 20, 2007), *available at* http://www.ftc.gov/os/caselist/0710170/071220statement.pdf.

[20] The complete transcripts of the Town Hall entitled *Ehavioral Advertising: Tracking, Targeting & Technology* are available at http://www.ftc.gov/bcp/workshops/ehavioral/71101wor.pdf and http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf.

[21] To facilitate a comprehensive discussion of the issues at the Ehavioral Advertising Town Hall, the FTC applied a broad definition of online behavioral advertising – namely, the collection of information about a consumer's online activities in order to deliver advertising targeted to the individual consumer's interests. This definition was meant to encompass the various tracking activities engaged in by diverse companies across the web. *See* Transcript of Town Hall Record at 8, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71101wor.pdf (introductory remarks of Lydia B. Parnes, Director, FTC Bureau of Consumer Protection) [hereinafter "Nov. 1 Transcript"]. FTC staff used a similar definition in its proposed Principles.

benefits to consumers in the form of free content, personalization that many consumers appear to value, and a potential reduction in unwanted advertising. Second, the invisibility of the practice to consumers raises privacy concerns, as does the risk that data collected for behavioral advertising – including sensitive data about children, health, or finances – could be misused. Third, business and consumer groups alike expressed support for transparency and consumer control in the online marketplace.[22]

A number of Town Hall participants also criticized existing self-regulatory efforts. Specifically, these participants stated that the NAI Principles had not been effective to address the privacy concerns that online behavioral advertising raises. They argued that the NAI Principles were too limited because they applied only to network advertisers and not to other business models. Other critics cited the purported lack of enforcement of the NAI Principles and its cumbersome and inaccessible opt-out system.[23] Further, while various industry associations discussed their online self-regulatory schemes to address privacy issues, these schemes did not generally focus on behavioral advertising.[24]

---

[22] Many similar issues arose during the FTC Town Hall held in May 2008 on the mobile commerce marketplace. There, participants discussed consumers' ability to control mobile marketing applications, the challenges of effective disclosures given the size limitations in the mobile context, marketing to sensitive groups, and the developments of the next generation of mobile-based products and services. *See generally* FTC Town Hall, *Beyond Voice: Mapping the Mobile Marketplace* (May 6-7, 2008), *available at* http://www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

[23] *See, e.g.*, Transcript of Town Hall Record at 144-149, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/71102wor.pdf (statements of Pam Dixon, Executive Director, World Privacy Forum) [hereinafter "Nov. 2 Transcript"].

[24] *Id.* at 135-143, 155-159. As an alternative to the existing self-regulatory models, and in an effort to increase consumers' control over the tracking of their online activities, a coalition of privacy groups proposed the development of a "Do Not Track List." *See* Ari Schwartz, CDT,

C. Staff's Proposed Self-Regulatory Principles

In response to the issues raised at the Town Hall, and to continue the dialogue with interested parties, in December 2007 Commission staff released the proposed self-regulatory Principles for public comment. Staff supported self-regulation because it provides the necessary flexibility to address evolving online business models. At the same time, however, staff recognized that existing self-regulatory efforts had not provided comprehensive and accessible protections to consumers. Accordingly, in issuing the proposed Principles, staff intended to guide industry in developing more meaningful and effective self-regulatory models than had been developed to date.

The proposed Principles include four governing concepts. The first is transparency and control: companies that collect information for behavioral advertising should provide meaningful disclosures to consumers about the practice and choice about whether to allow the practice. The second principle proposes reasonable security and limited data retention: companies should provide reasonable data security measures so that behavioral data does not fall into the wrong hands, and should retain data only as long as necessary for legitimate business or law enforcement needs. The third principle governs material changes to privacy policies: before a company uses behavioral data in a manner that is materially different from promises made when the company collected the data, it should obtain affirmative express consent from the

---

et al., *Consumer Rights and Protections in the Behavioral Advertising Sector, available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf (Oct. 31, 2007) (the proposed "Do Not Track List" is modeled after the FTC's national "Do Not Call" registry and would require online advertisers using a persistent identifier to provide to the FTC the domain names of the servers or other devices placing the identifier).

consumer.[25] The fourth principle states that companies should obtain affirmative express consent before they use sensitive data – for example, data about children, health, or finances – for behavioral advertising.[26] Finally, staff's proposal requested additional information regarding the potential uses of tracking data other than for behavioral advertising, including whether such secondary uses raise concerns and merit heightened protection.

D. Recent Initiatives to Address Privacy Concerns

Following the Town Hall and the release of the Principles, various individual companies, industry organizations, and privacy groups have taken steps to address some of the concerns and issues raised by online behavioral advertising. For example, a number of companies have developed new policies and procedures to inform consumers about online tracking and provide additional protections and controls over the practice.[27] In particular, both Google and Yahoo! Inc. ("Yahoo!") have announced new tools that will allow consumers to opt out of receiving targeted online advertisements.[28] Microsoft Corporation has announced that the new version of

---

[25] *See, e.g., In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf (alleging that the company made material changes to its privacy policy and applied such changes to data collected under the old policy). The FTC's order requires Gateway to obtain opt-in consent for such changes in the future.

[26] Staff recommended that companies obtain consumers' affirmative express consent for material, retroactive changes and for the use of sensitive data because of the increased privacy concerns raised by the collection and use of such data.

[27] FTC staff encourages continued stakeholder efforts to address the privacy concerns raised by behavioral advertising, but does not endorse any of the specific approaches described herein.

[28] *See* Press Release, Yahoo!, *Yahoo! Announces New Privacy Choice for Consumers* (Aug. 8, 2008), *available at* http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=327212; Posting of Rajas Moonka, Senior Business Product Manager, Google, to

its Internet browser will include a tool that, when enabled by a user, will not save browsing and searching history, cookies, form data, or passwords, and will automatically clear the browser cache at the end of each session.[29] Other steps include educational programs to inform consumers about online tracking[30] and new policies to reduce the length of time companies store personal data collected about online searches.[31]

In December 2008, in response to the criticism of the NAI Principles at the Town Hall and the FTC's call for stronger self-regulation, the NAI issued revised principles ("NAI 2008 Principles").[32] Although NAI has strengthened certain aspects of its self-regulatory regime –

---

http://googleblog.blogspot.com/2008/08/new-enhancements-on-google-content.html (Aug. 7, 2008, 5:01 EST).

[29] *See* Gregg Keizer, *Microsoft Adds Privacy Tools to IE8*, COMPUTERWORLD.COM, Aug. 25, 2008, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113419. As noted above, a coalition of privacy groups also has proposed and continues to support development of a "Do Not Track List" designed to increase consumer control over the tracking of their online activities. *See* Schwartz et al., *supra* note 24.

[30] *See* AOL, Privacy Gourmet Page, http://corp.aol.com/o/mr-penguin/ (last visited Jan. 9, 2009); YouTube, Google Search Privacy Playlist, http://www.youtube.com/view_play_list?p=ECB20E29232BCBBA (last visited Jan. 9, 2009).

[31] *See* Posting of Kim Hart, washingtonpost.com, to http://voices.washingtonpost.com/posttech/2008/12/yahoo_changes_data-retention_p.html?nav=rss_blog (Dec. 17, 2008, 13:50 EST) (stating that Yahoo! agreed to shorten online behavioral data retention periods from thirteen to three months); Posting of Stacey Higginbotham, GigaOM, to http://gigaom.com/2008/09/09/in-online-privacy-fight-google-blinks/ (Sept. 9, 2008, 7:47 PT) (stating that Google agreed to reduce storage of search engine inquiries from eighteen to nine months); *see also Microsoft to Cut Search Engine Data Retention to Six Months if Others Follow*, 7 PRIVACY & SEC. LAW REP. 1767 (2008) (stating that Microsoft announced it would reduce search engine data retention to six months in the European Union if all search companies agreed to do the same).

[32] *See* NAI, *2008 NAI Principles Code of Conduct* (Dec. 16, 2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf [hereinafter "NAI 2008 Principles"]. In advance of issuing the NAI 2008 Principles,

most notably by dramatically increasing its membership – staff believes that NAI could do more to ensure the transparency of online behavioral advertising to consumers. Staff also notes that certain elements of NAI's revised approach have yet to be clarified through implementation guidelines, which NAI plans to issue in 2009.[33] More recently, a joint industry task force including marketing and industry trade associations, as well as the Council of Better Business Bureaus, announced a cooperative effort to develop self-regulatory principles to address privacy concerns related to online behavioral advertising.[34]

NAI issued proposed principles for public comment in April 2008. *See* NAI, *Draft 2008 NAI Principles* (Apr. 10, 2008), *available at* http://www.networkadvertising.org/networks/NAI_Principles_2008_Draft_for_Public.pdf. In some respects, NAI's proposed principles contained stronger protections than those announced in December. For example, NAI's original proposal prohibited the use of certain categories of sensitive information, including information about children, for behavioral advertising. As finalized, the NAI 2008 Principles would allow use of these categories of information so long as consumers (or parents, in the case of children) provide their consent.

[33] The NAI 2008 Principles expand the security and access requirements to cover data used for behavioral advertising, as well as data used for practices such as tracking the number of ads served at a particular website. They also restrict NAI members' use of behavioral advertising data to marketing purposes and require that members retain such data only as long as needed for legitimate business purposes or as required by law. FTC staff commends NAI's attempts to strengthen its principles through these and other steps. At the same time, staff notes that there are areas where NAI may continue to improve. For example, staff notes that the NAI 2008 Principles' approach to providing notice and choice generally mirrors NAI's previous approach – *i.e.*, members may continue to provide notice to consumers through website privacy policies. For the reasons discussed below, staff encourages companies engaged in online behavioral advertising to develop mechanisms that allow for prominent disclosure outside companies' existing privacy policies. Moreover, because the revisions tie some obligations to certain language (*e.g.*, "directly engaging" in behavioral advertising) that will be defined through future implementation guidelines, the impact of these obligations is currently unclear. Similarly, because NAI plans to issue further guidance regarding the policies and procedures governing its compliance reviews, questions remain as to whether these reviews, and any penalties that are ultimately imposed, will be adequate to ensure compliance.

[34] The initiative includes the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association, and the Interactive Advertising Bureau ("IAB"). *See* K.C. Jones, *Agencies to Self-Regulate Online Behavioral Ads*,

Several other organizations have also developed materials to assist online businesses in identifying and addressing privacy concerns raised by online behavioral advertising. For example, the Future of Privacy Forum – an advocacy group of privacy scholars, lawyers, and corporate officials – has launched an initiative to develop new ways to provide consumers with control over the use of their personal information for online behavioral advertising.[35] The Center for Democracy and Technology ("CDT") also recently released an assessment tool, developed in conjunction with internet companies and public interest advocates, to help online companies evaluate the consumer privacy implications of their online behavioral advertising practices and to create appropriate, meaningful privacy protections.[36] Finally, TRUSTe, a privacy seal organization, has issued a white paper reviewing the current online behavioral advertising environment and providing a checklist to assist online companies to address issues raised by online behavioral advertising, especially those concerning transparency.[37]

Congress has also expressed concern about the privacy issues raised by online behavioral

---

INFORMATIONWEEK, Jan. 13, 2009, http://www.informationweek.com/news/showArticle.jhtml?articleID=212900156. The IAB, an organization of companies engaged in online advertising, previously issued a set of privacy principles recommending that its member companies notify consumers about data collection practices and provide choice when appropriate. IAB, *Privacy Principles* (Feb. 24, 2008), *available at* http://www.iab.net/iab_products_and_industry_services/1421/1443/1464.

[35] *See* Kim Hart, *A New Voice in Online Privacy*, WASH. POST, Nov. 17, 2008, at A06, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/11/16/AR2008111601624.html?nav=hcmoduletmv.

[36] *See* CDT, *Threshold Analysis for Online Advertising Practices* (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf.

[37] *See* TRUSTe, *Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust*, *available at* http://www.truste.com/about/online_behavioral_advertising.php (last visited Feb. 3, 2009).

advertising. On July 9, 2008, the Senate Committee on Commerce, Science, and Transportation ("Senate Committee") held a hearing entitled "Privacy Implications of Online Advertising," which examined the online advertising industry and the impact of these practices on consumers' privacy.[38] Witnesses from the FTC,[39] consumer groups, and industry discussed both the methods of online behavioral advertising employed by industry and the government's role in protecting consumer privacy. The Senate Committee held a follow-up hearing on September 25, 2008, which focused on behavioral advertising in conjunction with Internet Service Providers ("ISPs").[40] Testifying at the second hearing, corporate officers representing Verizon Communications, Inc., AT&T Services, Inc., and Time Warner Cable expressed support for self-regulation by the various entities engaged in online behavioral advertising practices. Specifically, these representatives called for a requirement that companies obtain opt-in consent from consumers before collecting online information for behavioral advertising purposes.

---

[38] *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf37017.

[39] *See id.* (statement of Lydia Parnes, Director of the FTC Bureau of Consumer Protection).

[40] *Broadband Providers and Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 110th Cong. (2008), *available at* http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=778594fe-a171-4906-a585-15f19e2d602a. In the ISP-based behavioral advertising model, a consumer's online activities are collected directly from the consumer's ISP, rather than from the individual websites the consumer visits. This model, which is also often referred to as "deep packet inspection," could potentially allow targeting of ads based on substantially all of the websites a consumer visits, rather than simply a consumer's visits to, and activities within, a given network of websites. *See* Peter Whoriskey, *Every Click You Make*, WASH. POST, Apr. 4, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html.

The House Committee on Energy and Commerce ("House Committee"), and its Subcommittee on Telecommunications and the Internet ("Telecommunications Subcommittee"), also have been active in this area, focusing in particular on ISP-related practices. On July 17, 2008, the Telecommunications Subcommittee held a hearing entitled "What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies" that included testimony from industry, experts, and consumer groups.[41] Thereafter, on August 1, 2008, four members of the House Committee issued letters to thirty-four companies seeking information on their practices with respect to behavioral advertising.[42] The companies' responses are available online.[43]

These developments suggest that there is continuing public interest in the issues that behavioral advertising raises and increasing engagement by industry members in developing solutions.

---

[41] *What Your Broadband Provider Knows About Your Web Use: Deep Packet Inspection and Communications Laws and Policies: Hearing Before the H. Subcomm. on Telecomm. & the Internet*, 110th Cong. (2008), *available at* http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml.

[42] Letter from John D. Dingell, Chairman of the H. Comm. on Energy & Commerce, et al., to William Bresnan, Chairman & C.E.O. of Bresnan Communications, et al. (Aug. 1, 2008), *available at* http://energycommerce.house.gov/Press_110/110-ltr.080108.AOL-TILetters.pdf.

[43] H. Comm. on Energy & Commerce, Responses to Aug. 1, 2008 Letter to Network Operators Regarding Data Collection Practices, *available at* http://energycommerce.house.gov/Press_110/080108.ResponsesDataCollectionLetter.shtml (last visited Jan. 9, 2009). In light of concerns expressed by Congress and others, at least one high profile company suspended its plans to engage in ISP-based behavioral advertising. *See* Ellen Nakashima, *NebuAd Halts Plans For Web Tracking*, WASH. POST, Sept. 4, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html.

III. SUMMARY OF THE COMMENTS RECEIVED AND STAFF'S ANALYSIS

In response to the proposed Principles, FTC staff received sixty-three comments from interested parties; because some of the comments represent the views of multiple parties, a total number of approximately eighty-seven stakeholders participated in the comment process. FTC staff greatly appreciates the substantial work of the parties that submitted comments. The comments have helped to clarify the differing perspectives regarding how best to address the privacy issues that online behavioral advertising raises.

As a threshold matter, some commenters stated that FTC staff's call for self-regulation is unnecessary and that the Principles could interfere with a developing and rapidly changing marketplace.[44] Others concluded that the Principles do not go far enough and that sweeping legislation is necessary. Between these positions, a majority of the commenters expressed support for some form of self-regulation. Most commenters also identified certain aspects of the Principles that, in their view, raise important issues, merit more guidance, or should be changed.

Set forth below is a summary of the comments arranged by topic. This summary highlights and discusses the main points and positions represented by the comments as a whole. Also included are FTC staff's responses to these main points, along with additional guidance

---

[44] One trade association comment also suggested that self-regulation at the behest of a governmental entity such as the FTC cannot truly be self-regulatory. In addition, a newspaper association stated that applying the Principles to a newspaper's advertising-supported website would violate the First Amendment because it could affect the selection of content that is presented to the reader. In response, staff notes that the Commission has often called for, studied the effectiveness of, and made suggestions for improving self-regulatory schemes, and that such efforts do not implicate the First Amendment. *See, e.g.*, FTC Report, *Marketing Violent Entertainment to Children: A Fifth Follow-Up Review of Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries* 33 (Apr. 2007), *available at* http://www.ftc.gov/reports/violence/070412MarketingViolentEChildren.pdf; FTC Report, *Self-Regulation in the Alcohol Industry* 25 (June 2008), *available at* http://www.ftc.gov/os/2008/06/080626alcoholreport.pdf.

regarding the Principles. The key theme underlying this guidance is the need to balance the potential benefits of the various practices covered by the Principles against the privacy concerns the practices raise. Among other things, staff considered consumer expectations regarding the practices; the extent to which the practices are transparent; the potential for consumer harm; and the need to maintain vigorous competition in the online marketplace and avoid stifling innovation.

In providing this guidance, staff notes that nothing in the discussion is intended to preclude or discourage the implementation of responsible or "best" practices outside of the Principles. Staff also notes that some of the Principles closely parallel FTC law and policy, which continue to apply regardless of the scope or coverage of the Principles. For example, depending upon on the circumstances, a company whose practices fall outside the Principles may still be required to implement reasonable measures to address any privacy or security risks to consumers' information.[45] Similarly, regardless of the Principles, companies may not unilaterally alter their policies and use previously collected data in a manner that materially differs from the terms under which the data was originally collected.[46] Companies should also be mindful of the federal and state laws that may apply to their operations.

Finally, staff notes that the FTC's work in this area, including its commitment to engage the public on these issues, will continue beyond this Report. Although the comments provided considerable information about the various business models and policy issues surrounding

---

[45] *See supra* note 8 (citing FTC settlements requiring companies to implement reasonable information security programs to protect sensitive personal information).

[46] *See In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917comp0423047.pdf.

behavioral advertising, staff has ongoing questions about the precise operation of this marketplace, particularly as it continues to develop and evolve. In addition, much remains to be learned about consumers' awareness, attitudes, and understanding of the practices. Staff therefore will continue to examine the issues as the market develops and will propose additional actions as needed. Staff also intends, where appropriate, to initiate investigations of possible unfair or deceptive acts or practices in this area that would potentially violate Section 5 of the FTC Act.

A. The Principles' Scope

As proposed, the Principles apply broadly to companies engaged in online behavioral advertising, defined as tracking consumers' online activities in order to deliver advertising that is targeted to the individual consumers' interests. Numerous commenters addressed the Principles' scope – specifically, the Principles' applicability to different types of data and different advertising practices. These commenters emphasized three significant issues: the applicability of the Principles not only to the collection and use of personally identifiable information ("PII"), but also of non-personally identifiable information ("non-PII");[47] the applicability to "first party," or "intra-site," collection and use of data; and the applicability to online contextual advertising.

1. Applicability to Non-PII

A number of commenters, representing industry groups and individual companies, stated that because the Principles' definition of online behavioral advertising fails to distinguish

[47] Traditionally, PII has been defined as information that can be linked to a specific individual including, but not limited to, name, postal address, email address, Social Security number, or driver's license number. Non-PII includes anonymous data that, without more, cannot identify a specific person. *See, e.g.*, June 2000 Report, *supra* note 10, at 4 & n.14.

between PII and non-PII, the Principles apply too broadly. Claiming that there is little or no privacy interest in non-PII and a limited potential for harm, these commenters argued that the FTC should exclude such data from the Principles. The commenters also maintained that application of the Principles to non-PII would impose significant costs on business and could interfere with companies' ability to provide free online content to consumers.

Similarly, some commenters noted that non-PII has traditionally fallen outside the bounds of U.S. privacy laws and self-regulatory programs and that the Principles' inclusion of such data marks a departure from the Commission's current approach to privacy issues. Not all industry comments supported a bright line distinction between PII and non-PII, however. For instance, an individual company and a seal organization recommended that the Principles recognize a third category of data – *i.e.*, data that falls in between PII and non-PII. Another individual company noted that even information that is not considered personally identifying can raise privacy concerns.

In contrast to the majority of industry comments, a number of consumer and privacy groups expressed support for applying the Principles to data typically considered to be non-PII. Specifically, these commenters would apply the Principles to such data as Internet Protocol (IP) addresses,[48] cookie data, and other information that the commenters stated could allow a set of behaviors or actions to be associated with a particular individual or computer user, even if that individual is never identified by name.

Staff believes that, in the context of online behavioral advertising, the traditional notion of what constitutes PII versus non-PII is becoming less and less meaningful and should not, by

---

[48] An IP address is a numerical identifier assigned to a computer or device that connects to the Internet.

itself, determine the protections provided for consumer data. Indeed, in this context, the Commission and other stakeholders have long recognized that both PII and non-PII raise privacy issues,[49] a view that has gained even more currency in recent years for a number of reasons. First, depending on the way information is collected and stored, it may be possible to link or merge non-PII with PII. For example, a website might collect anonymous tracking data and then link that data with PII (*e.g.*, name, address) that the consumer provided when registering at the site. Second, with the development of new and more sophisticated technologies, it likely will become easier to identify an individual consumer based on information traditionally considered to be non-PII. For instance, although industry has traditionally considered most IP addresses to be non-PII, it soon may be possible to link more IP addresses to specific individuals.[50]

Third, even where certain items of information are anonymous by themselves, they can become identifiable when combined and linked by a common identifier. For example, a consumer's Internet activity might reveal the restaurants in the neighborhood where she eats, the stores at which she shops, the property values of houses recently sold on her block, and the

---

[49] *See, e.g.*, July 2000 Report, *supra* note 11, at 11 n.33 (majority of the Commission recommended online privacy legislation applicable to both PII and non-PII); NAI 2008 Principles, *supra* note 32, at 3, 7-8 (since 2000, Principles have provided protections for PII and non-PII); Dingell et al., *supra* note 42 (seeking information from 34 companies on all aspects of their online behavioral advertising practices, regardless of whether the practices implicated PII or non-PII).

[50] In recent years, portable devices with multiple built-in functionalities tied to individual consumers have proliferated. These include devices such as "smart" mobile phones that allow Internet access and email, as well as BlackBerrys and other similar tools. The explosion in the number of devices in use world-wide is rapidly exhausting the available IP addresses required for online connectivity. In order to accommodate this growing demand, the market is undergoing a transition to a new generation of IP addresses – "IPv6." IPv6 will dramatically increase the number of unique IP addresses. While improving connectivity, IPv6 will rely more heavily on static IP addresses, which can link an individual IP address to a particular device that is associated with a specific individual.

medical conditions and prescription drugs she is researching; when combined, such information would constitute a highly detailed and sensitive profile that is potentially traceable to the consumer. The storage of such data also creates the risk that it could fall into the wrong hands or be used later in combination with even richer, more sensitive, data.[51]

Fourth, in some circumstances, such as when more than one individual in a household shares or has access to a single computer, the distinction between PII and non-PII may have no bearing on the privacy risks at issue. For example, one user may visit a website to find information about a highly personal or sensitive topic, such as the user's health issues or sexual preference. In such circumstances, the delivery of advertising associated with that user's searches to the shared computer, even if the advertising does not identify the user, could reveal private information to another user of the same computer.

Finally, available evidence shows that consumers are concerned about the collection of their data online, regardless of whether the information is characterized as PII or non-PII. Recent survey data suggests that significant percentages of consumers are uncomfortable with

---

[51] This hypothetical is supported by the 2006 incident in which AOL made public some 20 million search queries conducted by thousands of subscribers over a three-month period. After replacing subscriber names or user IDs with identification numbers in order to protect the searchers' anonymity, AOL posted the data for research purposes. The data, which was posted for about a week, connected the "anonymized" AOL member with his or her search queries, the number of websites identified by AOL's search engine as responsive to the search queries, and the responsive website the individual chose to visit. Using this information, the media was able to identify, with little additional investigation, at least one individual subscriber and "bloggers" and other Internet users claimed to be able to identify others. *See, e.g.*, Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&scp=1&sq=aol%20queries&st=cse&oref=slogin; Ellen Nakashima, *AOL Takes Down Site With Users' Search Data*, WASH. POST, Aug. 8, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080701150.html.

having their online activities tracked for purposes of delivering advertisements, even where the data collected is not personally identifiable.[52] Further, many consumers reacted strongly to the AOL incident, described above, in which AOL made public purportedly anonymous data about its subscribers' online activities. Upon learning that the data had been posted online, these consumers expressed surprise and concern that the company stored data about their online activities – and stored it in a way that allowed the data to be associated, at least in some cases, with particular individuals.[53]

---

[52] *See, e.g.*, Press Release, Consumers Union, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy* (Sept. 25, 2008), *available at* http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html (over half of respondents uncomfortable with internet companies using their browsing histories to send relevant ads or third parties collecting information about their online behavior); Press Release, Harris Interactive Inc., *Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles* (Apr. 10, 2008), *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=894 (59% of survey respondents were "not comfortable" with online behavioral advertising; however, after being shown model privacy policies, 55% said they would be more comfortable); Press Release, TRUSTe, *TRUSTe Report Reveals Consumer Awareness and Attitudes About Behavioral Targeting* (Mar. 26, 2008), *available at* http://www.truste.org/about/press_release/03_26_08.php (57% of survey respondents "not comfortable" with advertisers using browsing history to serve relevant ads, even when information cannot be tied to their names or other personal information); George Milne, "Information Exchange Expectations of Consumers, Marketing Managers, and Direct Marketers" at 3, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3gmilne.pdf (45% of respondents think online tracking should not be permitted; 47% would permit tracking with opt-in or opt-out rights); *see also* Larry Ponemon, "FTC Presentation on Cookies and Consumer Permissions" at 11, *Ehavioral Advertising: Tracking, Targeting & Technology* (Nov. 1, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/presentations/3lponemon.pdf (only 20% of respondents would voluntarily permit marketers to share buying behavior with third parties to project future buying decisions).

[53] *See, e.g.*, *AOL is Sued Over Privacy Breach*, L.A. TIMES, Sept. 26, 2006, at C2, *available at* http://articles.latimes.com/2006/sep/26/business/fi-aol26; Barbaro & Zeller, Jr., *supra* note 51; Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch, Aug. 6, 2006, http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/all-comments/. The AOL incident highlights the difficulties in making data truly anonymous. Simply eliminating name, contact information, or

In staff's view, the best approach is to include within the Principles' scope any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device. Whether information "reasonably could be associated" with a particular consumer or device will depend on the factual circumstances and available technologies, but would include, for example: clickstream data that, through reasonable efforts, could be combined with the consumer's website registration information; individual pieces of anonymous data combined into a profile sufficiently detailed that it could become identified with a particular person; and behavioral profiles that, while not associated with a particular consumer, are stored and used to deliver personalized advertising and content to a particular device.[54] Such an approach will ensure protections for consumer data that raises a consumer privacy interest without imposing undue costs where data is truly anonymous and privacy concerns are minimal. As noted above, this is also consistent with NAI's approach, the predominant industry self-regulatory model, which has mandated protections for both PII and

---

other traditional PII may not be sufficient. For example, a study conducted in 2000 used U.S. Census summary data to find that 87% of the U.S. population could likely be uniquely identified based only on three pieces of data: a 5-digit zip code; gender; and date of birth. Latanya Sweeney, Abstract, *Uniqueness of Simple Demographics in the U.S. Population* (Carnegie Mellon U., Laboratory for Int'l Data Privacy 2000), *available at* http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html; *see also* Bruce Schneier, *Why "Anonymous" Data Sometimes Isn't*, WIRED, Dec. 13, 2007, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_1213 (describing University of Texas experiments with de-anonymized Netflix data); Latanya Sweeney, *Comments to the Department of Health and Human Services on "Standards of Privacy of Individually Identifiable Health Information"* (Apr. 26, 2002), *available at* http://privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.pdf (describing experiments on a state's anonymized cancer registry).

[54] As discussed below, staff has limited the scope of the Principles in several ways that also limit their application to data traditionally considered to be non-PII. *See* discussion *infra* Parts III.A.2 and 3.

non-PII since 2000.

2. Applicability to "First Party" Online Behavioral Advertising

The Principles' applicability to "first party," or "intra-site," online behavioral advertising also generated numerous comments, primarily from industry groups and individual companies. Most of these commenters objected to the Principles' application to behavioral advertising by, and at, a single website. Instead, they urged the Commission to limit the Principles to practices that involve the tracking of consumers' activities across different websites. These commenters argued that "first party" collection and use of consumer information is transparent and consistent with consumer expectations. Additionally, the commenters described a variety of services and operations, valued by consumers, that require "first party" data collection and use. These include product recommendations, tailored content, shopping cart services, website design and optimization, fraud detection, and security.

Some commenters, including an individual company and a seal organization, recognized that the tracking of consumers across multiple sites raises increased concern, but did not support excluding "first party" practices from self-regulation entirely. Other commenters, including an individual company and several consumer groups, generally supported the Principles' application to "first party" behavioral advertising.

After considering the comments, staff agrees that "first party" behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites. For example, under the "first party" model, a consumer visiting an online retailer's website may receive a recommendation for a product based upon the consumer's prior purchases or browsing activities at that site (*e.g.*, "based on your interest in travel, you might enjoy the

following books"). In such case, the tracking of the consumer's online activities in order to deliver a recommendation or advertisement tailored to the consumer's inferred interests involves a single website where the consumer has previously purchased or looked at items. Staff believes that, given the direct relationship between the consumer and the website, the consumer is likely to understand why he has received the targeted recommendation or advertisement and indeed may expect it. The direct relationship also puts the consumer in a better position to raise any concerns he has about the collection and use of his data, exercise any choices offered by the website, or avoid the practice altogether by taking his business elsewhere. By contrast, when behavioral advertising involves the sharing of data with ad networks or other third parties, the consumer may not understand why he has received ads from unknown marketers based on his activities at an assortment of previously visited websites. Moreover, he may not know whom to contact to register his concerns or how to avoid the practice.

In addition, staff agrees that "first party" collection and use of consumer data may be necessary for a variety of consumer benefits and services. These include not only personalized content and other elements of the interactive online experience that consumers may value, but also important internal functions such as security measures, fraud prevention, and legal compliance.[55]

Finally, maintaining data for internal use only also limits the risk that the data will fall into the wrong hands. For that reason, privacy schemes in varied contexts have distinguished between a site's internal use of data and the sharing of data with third parties, imposing stronger

---

[55] Staff notes that to the extent that these functions do not involve the tracking of consumers' online activities in order to deliver advertising based on those activities, they do not constitute online behavioral advertising and thus already fall outside the Principles' scope.

privacy protections for the latter.[56] Staff believes that the same distinction holds true here.

Based on these considerations, staff agrees that it is not necessary to include "first party" behavioral advertising practices within the scope of the Principles.[57] If a website collects and then sells or shares data with third parties for purposes of behavioral advertising,[58] or participates in a network that collects data at the site for purposes of behavioral advertising, however, such practices would remain within the scope of the Principles.[59]

---

[56] For instance, the Children's Online Privacy Protection Rule ("COPPA Rule") recognizes that sharing of children's personal information with third parties raises more concern than use of the information simply for internal purposes. For this reason the COPPA Rule requires that website operators obtain the highest level of verifiable parental consent where such information is shared and, where possible, that the website enable parents to choose whether to allow sharing. *See* 16 C.F.R. § 312.4 (2006); Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,899 (Nov. 3, 1999), *available at* http://www.ftc.gov/os/1999/10/64fr59888.pdf. *See also* Direct Marketing Assocation ("DMA"), *Direct Marketing Association's Online Marketing Guidelines and Do the Right Thing Commentary* (Jan. 2002), *available at* http://www.the-dma.org/guidelines/onlineguidelines.shtml (recommending choice when data is shared with third parties).

[57] Staff notes that some of the principles are based on existing Commission case law and policy. As such, a company engaged in first party practices may still be required to provide reasonable security for the consumer data it collects and maintains. Additionally, depending upon the specific circumstances, a company may be precluded from using previously collected data in a way that conflicts with the privacy promises in effect at the time the company collected the data.

[58] To the extent that websites share data with third-party service providers in order to deliver ads or perform some of the internal functions described above, such sharing will still be considered "first party" use, provided there is no further use of the data by the service provider.

[59] Several commenters argue that data collection and use within a family of websites – *e.g.*, sites under common ownership or control – should be considered "first party" for purposes of the Principles. The commenters stated that consumers will save costs due to partnering arrangements, that consumers expect and want the additional marketing opportunities created through data sharing among affiliated websites, and that the Gramm-Leach-Bliley Act (the "GLB Act") allows financial institutions to share data with affiliates.

Staff believes that whether data sharing among affiliated companies should be considered "first party," and thus outside the scope of the Principles, should turn on whether the relationship among the sites – and the possibility that they may share data – is sufficiently transparent and

3. Applicability to Contextual Advertising

Numerous commenters, representing both industry and consumer groups, recommended that the Commission revise the Principles' behavioral advertising definition to expressly exclude contextual advertising. These commenters explained that online contextual advertising differs from behaviorally targeted advertising because it is based only on the content of a particular website or search query, rather than on information about the consumer collected over time. For example, where a consumer is shown an advertisement for tennis rackets solely because he is visiting a tennis-focused website or has used a search engine to find stores that sell tennis rackets, the advertisement is contextual.

The commenters described contextual advertising as transparent and consistent with consumers' expectations, similar to the "first party" practices discussed above. They also stated that, rather than being surprised by the practice, consumers expect and want to receive an ad for a product or service when visiting a website that is related to that product or service. Additionally, a number of commenters noted that contextual advertising creates fewer risks to privacy because the practice does not rely on the collection of detailed information about the consumer's actions over time. One group of consumer and privacy advocates also stated that excluding contextual advertising from the Principles may provide companies with an incentive to store less data about consumers.

---

consistent with reasonable consumer expectations. For instance, although one might expect that Citibank and Citifinancial are closely linked entities, the link between affiliates Smith Barney and Citibank is likely to be much less obvious. Such a determination will depend upon the particular circumstances. Staff also notes that the GLB Act does not, in fact, address affiliate sharing among financial institutions; rather, the Fair Credit Reporting Act governs affiliate sharing and allows consumers to opt out of sharing certain data with affiliates. *See* 15 U.S.C. §§ 1681a(d)(2)(A), 1681s-3 (2003).

In general, the comments described online contextual advertising as the delivery of ads based upon a consumer's current visit to a single web page or a single search query, without the collection and retention of data about the consumer's online activities over time. Based on this description, staff agrees that contextual advertising provides greater transparency than other forms of behavioral advertising, is more likely to be consistent with consumer expectations, and presents minimal privacy intrusion when weighed against the potential benefits to consumers. As discussed above, these benefits may include free content – made possible by the revenue from the sale of the advertisements – and receipt of contextually relevant ads that consumers may value. Staff consequently does not believe that it is necessary for the Principles to cover this form of online advertising.[60] It should be stressed that, based on the comments and other considerations, staff has defined contextual advertising narrowly. Where a practice involves the collection and retention of consumer data for future purposes beyond the immediate delivery of an ad or search result, the practice does not constitute contextual advertising.

B. Transparency and Consumer Control

Numerous commenters – including individual consumers, industry representatives, and consumer and privacy advocates – discussed the first proposed principle, which calls for greater transparency and consumer control of online behavioral advertising practices. Specifically, FTC staff proposed that websites where data is collected for behavioral advertising should provide prominent notice to consumers about such practices and should also offer consumers the ability to choose whether to allow such collection and use. In discussing this principle, commenters

---

[60] As discussed with respect to first party practices, companies engaged in online contextual advertising may still be subject to laws and policies that impose obligations outside of the Principles. *See supra* note 57.

focused primarily on two issues: whether to provide choice for the collection and use of non-PII, and how best to provide disclosures about the practices.

1. Choice for Non-PII

The commenters generally agreed that companies should notify consumers when they are collecting information about consumers' online activities for behavioral advertising. Indeed, several commenters noted that existing self-regulatory regimes currently require such notice.[61] Some industry trade groups and an individual company, however, stated that the first principle goes too far in proposing *choice* for the collection of non-PII. In general, these commenters made the same arguments with respect to choice for non-PII that are discussed above with respect to the overall scope of the Principles: that choice for non-PII is inconsistent with existing self-regulatory privacy schemes and laws; that there is a reduced privacy interest in, and risk of harm from, non-PII; and that choice will interfere with the free content and other benefits that online behavioral advertising offers. Some commenters also noted that consumers already have the ability to choose not to conduct business with websites that collect their data. These commenters suggested that consumers do not own the data that websites collect about them, and that there is no precedent for giving consumers the ability to dictate the terms upon which they use a website.[62]

---

[61] These commenters cited self-regulatory regimes such as DMA's "Online Marketing Guidelines," IAB's "Interactive Advertising Privacy Principles," and the NAI Principles.

[62] Some commenters also state that encouraging companies to provide choice for the mere *collection* of data is inconsistent with existing legal and self-regulatory regimes, which focus on choice in connection with particular *uses* of data. In fact, the Principles focus on the collection of data *for behavioral advertising*, which presumes both collection and use (or at least intended use) for that purpose. Further, the central goal of the Principles is to minimize potential misuses of data, including uses of data that could cause harm or are contrary to consumer expectations. Nevertheless, because many of the privacy concerns raised about behavioral

In contrast, various consumer and privacy interest groups, as well as a number of individual consumers, supported the concept of choice for the collection and use of non-PII for behavioral advertising and several asserted that the principle should go even further. Some of these commenters called for an *opt-in* choice[63] before data is collected and recommended that consumers receive clear notice about the purpose for which their data is collected. A coalition of consumer groups described the principle as inadequate and recommended the "Do Not Track" registry to allow consumers to limit online tracking.[64] Individual consumers also submitted comments expressing support for notice and the ability to control whether to allow collection of information about their online activities. One consumer stated that companies should be required to obtain permission to collect data regardless of how they use it.

For the reasons discussed above with respect to the Principles' overall scope, FTC staff believes that companies should provide consumer choice for the collection of data for online behavioral advertising if the data reasonably could be associated with a particular consumer or with a particular computer or device. As noted, the line separating PII and non-PII has become increasingly indistinct, and the predominant industry self-regulatory program has already adopted an approach that protects both types of information. Available research also suggests

---

advertising relate directly to information *collection* – including the invisibility of the practice and the risk that sensitive data, once collected, could fall into the wrong hands – staff believes that it is important to protect the data at the time of collection.

[63] The proposed Principles do not specify whether this choice would be opt-in or opt-out choice – just that it be clear, easy-to-use, and accessible to consumers. As discussed below, however, the Principles do specify affirmative express consent (opt-in) for uses of data that raise heightened privacy concerns – specifically, material changes affecting the use of previously collected data and the use of sensitive consumer data.

[64] *See supra* note 24.

that consumers are concerned about their data collected online, regardless of whether it is characterized as PII or non-PII. Finally, because staff has clarified that the Principles do not cover "first party" and "contextual" advertising, the costs of providing choice should be significantly less than stated in some comments.

2. Providing Effective Notice and Choice

Many commenters also addressed the issue of *how* businesses engaged in behavioral advertising should notify and offer choice to consumers concerning the collection and use of their data. Several companies stated that the appropriate location for any disclosure regarding online behavioral advertising is the website's privacy policy, and suggested that additional or alternative mechanisms for such disclosures could confuse consumers or encumber online functions. These commenters argued that consumers expect to find information on data practices in privacy policies and that this existing framework effectively informs consumers. Other companies and some privacy advocates highlighted the need for additional disclosure mechanisms beyond the privacy policy and suggested various options, such as: (i) providing "just-in-time" notice at the point at which a consumer's action triggers data collection; (ii) placing a text prompt next to, or imbedded in, the advertisement; and (iii) placing a prominent disclosure on the website that links to the relevant area within the site's privacy policy for a more detailed description.

A number of consumer and privacy groups' comments focused on the content of the disclosures and suggested that, in order for notice and consent to be effective, websites should not only disclose that information is collected, but should also specify the type of information collected, its uses, how long it will be retained, and with whom it will be shared. Other commenters – including an individual consumer and an online advertising company – suggested

that the use of standard or uniform disclosures would make disclosures more effective and would increase consumers' understanding of data collection practices. A group of privacy and consumer advocates recommended that, where a consumer opts out of behavioral advertising, companies should honor that choice until the consumer decides to opt in and should not attempt to circumvent the consumer's choice through technological means. These commenters also called on companies to allow consumers to view and change their choices at any time.

Another comment, filed by two academics, discussed the inherent problem with using cookies both to track consumers' online activities[65] and to record consumers' choice of whether to allow such tracking. These commenters noted that where consumers take steps to control the privacy of their online activities, through the use of anti-spyware software or by deleting cookies from their computer browsers, the consumers may unintentionally also block or delete the cookies that record their behavioral advertising preference. The commenters suggested possible solutions to this problem, including the development of standards for distinguishing between opt-out cookies and other types of cookies and modifying browser settings to give consumers greater control over their cookies.

Several companies also requested guidance regarding the form and content of notice in different contexts – such as on mobile devices, on "Web 2.0," and through ISPs – and questioned whether a uniform or standard approach can be created. For example, commenters raised questions regarding the mechanics of providing notice and choice in the Web 2.0 world, where a consumer may use several different third-party applications on a single, unrelated host web page. Some commenters raised issues regarding appropriate notice in the mobile context. Others

---

[65] *See supra* note 3.

stated that, as proposed, the transparency and control principle would exclude certain business models, including where an ISP collects, or allows a third party to collect, consumers' online data.[66] With respect to ISP-based behavioral advertising, these commenters recommended that the principle permit notice through direct communication from the ISP to its subscribers rather than on a website.

The differing perspectives on how best to provide consumers with effective notice and choice highlight the complexities surrounding this issue. Staff recognizes that it is now customary to include most privacy disclosures in a website's privacy policy. Unfortunately, as noted by many of the commenters and by many participants at the FTC's November 2007 Town Hall, privacy policies have become long and difficult to understand, and may not be an effective way to communicate information to consumers.[67] Staff therefore encourages companies to design innovative ways – outside of the privacy policy – to provide behavioral advertising disclosures and choice options to consumers.

A number of the commenters' recommendations appear promising. For example, a disclosure (*e.g.*, "why did I get this ad?") that is located in close proximity to an advertisement

---

[66] Specifically, one commenter noted that, where data about a consumer's online activities is collected through the ISP rather than from individual websites that the consumer visits (*see* discussion *supra* note 40), the company collecting the data does not have a direct relationship with the websites. Therefore, the company is not in a position to require the sites to provide consumers with notice and choice about data collection and use for behavioral advertising. Consequently, this commenter suggested that the Principles should contemplate notice and choice mechanisms outside the website context.

[67] *See, e.g.*, Jon Leibowitz, Commissioner, FTC, Remarks at the FTC Town Hall Meeting on "Ehavioral Advertising: Tracking, Targeting, & Technology" at 4-5 (Nov. 1, 2007), *available at* http://www.ftc.gov/speeches/leibowitz/071031ehavior.pdf; Nov. 1 Transcript, *supra* note 21, at 200-253 (Session 5: Roundtable Discussions of Data Collection, Use and Protection); Nov. 2 Transcript, *supra* note 23, at 9-94 (Session 6: Disclosures to Consumers).

and links to the pertinent section of a privacy policy explaining how data is collected for purposes of delivering targeted advertising, could be an effective way to communicate with consumers. Indeed, such a disclosure is likely to be far more effective than a discussion (even a clear one) that is buried within a company's privacy policy. Further, as described above, some businesses have already begun to experiment with designing other creative and effective disclosure mechanisms. Staff encourages these efforts and notes that they may be most effective if combined with consumer education programs that explain not only what information is collected from consumers and how it is used, but also the tradeoffs involved – that is, what consumers obtain in exchange for allowing the collection and use of their personal information.

With respect to the concern about using cookies to allow consumers to exercise their control over whether to allow behavioral advertising, staff encourages interested parties to examine this issue and explore potential standards and other tools to assist consumers. Moreover, as to some commenters' call for guidance on the mechanics of disclosures outside the website context, staff notes that different business models may require different types of disclosures and different methods for providing consumer choice. Staff therefore calls upon industry to develop self-regulatory regimes for these business models that effectively implement the transparency and consumer control principle. Regardless of the particular business model involved, the disclosures should clearly and prominently inform consumers about the practice and provide them with meaningful, accessible choice.

Finally, staff notes that research suggests that it is important to test proposed disclosures to ensure that they serve their intended purpose.[68] Staff therefore encourages stakeholders to

---

[68] *See, e.g.*, FTC Bureau of Economics Staff Report, *Improving Consumer Mortgage Disclosures: An Empirical Assessment of Current and Prototype Disclosure Forms* (June 2007),

conduct empirical research to explore the effects of possible disclosures on consumer understanding in this area.

C. Reasonable Security and Limited Data Retention for Consumer Data

Commenters also discussed the second proposed principle, which calls upon companies to provide reasonable security for, and limited retention of, consumer data collected for behavioral advertising purposes.

A number of companies generally supported this principle as drafted. Echoing the arguments raised about the Principles' applicability to non-PII, other companies, as well as industry groups, recommended that the Commission limit the application of this principle to PII. These commenters also called for more flexibility in applying this principle, and stated that data retention should not constitute a separate, stand-alone principle; instead, according to these commenters, data retention should be viewed as one possible component of an effective security program. Several industry commenters suggested that the principle should allow companies to consider various factors in evaluating appropriate data retention periods, and should refrain from imposing a uniform requirement.

Although the consumer groups generally supported this principle as proposed, some argued that the FTC should strengthen certain aspects of the principle. Individual consumers and one privacy group suggested that the principle is too vague and should provide more detailed and precise security standards. Two privacy groups stated that companies should retain data only as long as needed to fulfill the identified use for which the company collected the data. Other

---

available at http://www.ftc.gov/os/2007/06/P025505MortgageDisclosureReport.pdf; Kleimann Comm. Group, Inc., *Evolution of a Prototype Financial Privacy Notice: A Report on the Form Development Project* (Feb. 28, 2006), *available at* http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf.

proposals included a requirement that companies anonymize all retained data, a requirement that data be retained for no longer than six months, and a suggestion that the FTC hold a workshop to explore issues related to the appropriate data retention standard.

For the reasons addressed above, staff believes the Principles should apply to all data collected and used for behavioral advertising that reasonably could be associated with a particular consumer or with a particular computer or device. Staff recognizes, however, that there is a range of sensitivities within this class of data, with the most sensitive data warranting the greatest protection. Accordingly, as proposed, the data security principle stated that, consistent with existing data security laws and the FTC's many data security enforcement actions,[69] the "protections should be based on the sensitivity of the data [and] the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company." Staff believes that this scalable standard addresses the commenters' concerns while also ensuring appropriate protections for consumer data. Staff therefore retains this language in the Principles without change.

Staff agrees with many of the commenters, however, that data retention is one component in the reasonable security calculus, rather than a separate, stand-alone principle, and has clarified the principle to reflect this position. The intent behind the principle remains unchanged, however: companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. As noted above, over the past year some companies have changed their data retention policies to reduce substantially the length of time they maintain

---

[69] *See, e.g.*, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2002). Information about the FTC's data security program and enforcement actions can be found at http://www.ftc.gov/privacy/.

information about consumers' online activities. Staff commends such efforts.

D. Affirmative Express Consent for Material Retroactive Changes to Privacy Promises

Many commenters discussed the material change principle, which calls upon companies to obtain affirmative express consent before they use data in a manner that is materially different from the promises the company made at the time of collection. A number of industry commenters objected to this principle as proposed. These commenters called for more flexibility so that companies, in determining the type of notice and choice to offer consumers, can take into account the type of data affected and its sensitivity. The commenters argued that requiring notice and opt-in choice for material changes with respect to all types of data is not only unnecessary, but also is technologically unworkable, and could cause consumer confusion and inconvenience. Additionally, several of these commenters stated that, as proposed, this principle goes beyond FTC case law and existing self-regulatory regimes and statutes. Other commenters expressed concern that this principle will be applied to prospective changes to companies' practices and noted that such changes should, at most, require opt-out consent.

By contrast, consumer and privacy groups, as well as an individual consumer, expressed strong support for this principle as proposed. One consumer organization acknowledged that a business may have legitimate reasons for altering its privacy promises and stated that the principle strikes the proper balance between consumers' interests in reliable promises and industry's need for flexibility. This commenter expressed concern, however, about the use of "pre-checked" boxes and similar mechanisms to obtain opt-in consent, and noted that such

mechanisms might not reflect consumers' actual intent.[70]

It is fundamental FTC law and policy that companies must deliver on promises they make to consumers about how their information is collected, used, and shared.[71] An important corollary is that a company cannot use data in a manner that is materially different from promises the company made when it collected the data without first obtaining the consumer's consent.[72] Otherwise, the promise has no meaning. Staff recognizes, however, that a business may have a legitimate need to change its privacy policy from time to time, especially in the dynamic online marketplace. In addition, minor changes to a company's data practices may be

---

[70] Staff agrees that pre-checked boxes and choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement are insufficient to express a consumer's "affirmative express consent." *See, e.g.*, Deborah Platt Majoras, Chairman, FTC, Remarks at the Anti-Spyware Coalition at 7 (Feb. 9, 2006), *available at* http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf ("[B]urying critical information in the End User License Agreement ("EULA") does not satisfy the requirement for clear and conspicuous disclosure. Buried disclosures do not work."); FTC Publication, *Dot Com Disclosures: Information About Online Advertising* at 5 (May 2000), *available at* http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf ("Making [a] disclosure available . . . so that consumers who are looking for the information *might* find it doesn't meet the clear and conspicuous standard . . . . [D]isclosures must be communicated effectively so that consumers are likely to notice and understand them.") (emphasis in original); *see also* FTC Policy Statement on Deception at Part III, appended to *In the Matter of Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm (fine print disclosures not adequate to cure deception).

[71] *See, e.g.*, *FTC v. Toysmart.com, LLC*, No. 00-11341-RGS (D. Mass. filed July 10, 2000) (alleging that company violated privacy promises); *In the Matter of Life is good, Inc.*, FTC Docket No. C-4218 (Apr. 16, 2008) (alleging that company violated promises about the security provided for customer data); *In the Matter of Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005) (same); *In the Matter of MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) (same); *In the Matter of Educ. Research Ctr. of Am.*, FTC Docket No. C-4079 (May 6, 2003) (alleging that company violated privacy promises); *In the Matter of Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002) (alleging that company violated privacy and security promises).

[72] *See, e.g.*, *In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004); *see also In the Matter of Orkin Exterminating Co.*, 108 F.T.C. 263 (1986).

immaterial to consumers and may not warrant the costs and burdens of obtaining consumers' consent.

For these reasons, the material change principle is limited to changes that are both *material*[73] and *retroactive.* Depending upon a company's initial privacy promises, a material change could include, for example: (i) using data for different purposes than described at the time of collection, or (ii) sharing data with third parties, contrary to promises made at the time of collection. A retroactive change is a change in a company's policies or practices that a company applies to previously collected data. This would include, for example, the situation where a company makes a material change to its privacy policy and then uses previously collected data in a manner consistent with the new policy, but not the old one. A retroactive change does not include the circumstance where a company changes its privacy policy and then proceeds to collect and use *new* data under the new policy. Staff agrees that the latter type of change – which would constitute a *prospective* change – may not raise the same concerns as a retroactive change, and may therefore call for a more flexible approach.[74]

Staff has revised the material change principle to make clear that it applies to retroactive

---

[73] Under Commission law and policy, the term "material" refers to whether a practice, or information about a practice, is likely to affect a consumer's conduct or decisions with regard to a product or service. *See* FTC Policy Statement on Deception, *supra* note 70, at Part IV. Similarly, a "material change" refers to a change in a company's practices that, if known to the consumer, would likely affect the consumer's conduct or decisions with respect to the company's products or services.

[74] Many companies provide some form of prominent notice and opt-out choice for prospective changes – by sending an email notice to their customers, for example, or providing a prominent notice on the landing page of their website. Depending on the circumstances, such an approach may be sufficient. Of course, in deciding how to address prospective material changes, companies must consider such factors as: what claims were made in the original privacy policy, the sensitivity of the information at issue, and the need to ensure that any repeat visitors to a website are sufficiently alerted to the change.

changes only.

E. Affirmative Express Consent to (or Prohibition Against) Use of Sensitive Data

The fourth principle states that companies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer to receive the advertising. Many of the commenters who discussed this principle raised the issue of how to define the types of information that should be considered sensitive. Some commenters also questioned whether affirmative express consent is the appropriate standard or whether behavioral advertising based on sensitive data should be prohibited altogether.

Various commenters discussed the lack of agreement regarding the definition of "sensitive," and noted that whether specific information is considered sensitive can depend upon the context and the individual consumer's perspective. Other comments – including those filed on behalf of scientific and medical organizations, industry groups, and privacy and consumer advocates – listed specific categories of information that should be considered sensitive. According to these commenters, the categories include information about children and adolescents, medical information, financial information and account numbers, Social Security numbers, sexual orientation information, government-issued identifiers, and precise geographic location.[75]

Despite the lack of agreement on the definition of "sensitive data," there appears to be consensus that such data merits some form of heightened protection. Different commenters,

---

[75] The sensitivity of precise geographic location information was also discussed at a panel on mobile "location-based services" during the FTC's 2008 Town Hall on mobile marketing. *See* Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace* (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

however, provided differing views on the necessary level of protection. Several individual companies and industry groups objected to an opt-in approach. These commenters stated that opt-in consent for the collection of sensitive data for online behavioral advertising is too burdensome and is unnecessary in light of existing regulatory regimes.[76] Others stated that the uncertainty over how to classify sensitive data makes an opt-in approach difficult to implement and enforce.

Another group of commenters, including business and consumer groups, supported an affirmative express consent standard for certain sensitive data. They reasoned that such a standard strikes the correct balance and would allow those consumers who value advertising based on sensitive information to receive it.

A third group of commenters, including individual consumers, businesses, consumer groups, and a state government agency, supported a ban on behavioral advertising based on sensitive data. These commenters cited the risk of harm from sensitive data falling into the wrong hands. Other commenters recommended banning the use of specific types of sensitive data, such as information about children. Finally, a number of commenters called for additional examination of the issue, including discussion about how to define what constitutes sensitive data.

Given the heightened privacy concerns and the potential for significant consumer harm from the misuse of sensitive data, staff continues to believe that affirmative express consent is

---

[76] These commenters specifically cited the COPPA Rule (children's information), the Health Insurance Portability and Accountability Act ("HIPAA") (health information), and the GLB Act (financial information).

warranted.[77] Indeed, this protection is particularly important in the context of online behavioral advertising, where data collection is typically invisible to consumers who may believe that they are searching anonymously for information about medications, diseases, sexual orientation, or other highly sensitive topics. Moreover, contrary to the suggestions in the comments, existing statutory regimes do not address most types of online behavioral advertising or the privacy concerns that such advertising raises.

With respect to defining what constitutes sensitive data, staff agrees with the commenters that such a task is complex and may often depend on the context. Although financial data, data about children, health information, precise geographic location information, and Social Security numbers are the clearest examples, staff encourages industry, consumer and privacy advocates, and other stakeholders to develop more specific standards to address this issue. Staff also encourages stakeholders to consider whether there may be certain categories of data that are so sensitive that they should never be used for behavioral advertising.

F. Secondary Uses

Relatively few commenters responded to the Principles' call for information regarding the use of tracking data for purposes other than behavioral advertising. Most of the industry commenters that did address this question focused on such internal uses as website design and optimization, content customization, research and development, fraud detection, and security. For the reasons discussed above, staff believes that such "first party" or "intra-site" uses are unlikely to raise privacy concerns warranting the protections of the Principles. Other businesses

---

[77] As discussed previously, *supra* note 70, pre-checked boxes or disclosures that are buried in a privacy policy or a uniform licensing agreement are unlikely to be sufficiently prominent to obtain a consumer's "affirmative express consent."

and some consumer groups cited potential harmful secondary uses, including selling personally identifiable behavioral data, linking click stream data to PII from other sources, or using behavioral data to make credit or insurance decisions. These commenters noted, however, that such uses do not appear to be well-documented. Some commenters recommended that the FTC seek more information regarding secondary uses, including the extent to which the collection of data by third-party applications operating on a host website constitutes secondary use.

Given the dearth of responses to staff's request for specific information, it is unclear whether companies currently use tracking data for non-behavioral advertising purposes other than the internal operations identified above.[78] Staff therefore does not propose to address this issue in the Principles at this time. Staff agrees with some of the commenters, however, that the issue of secondary use merits additional consideration and dialogue. Therefore, as staff continues its work on behavioral advertising, it will seek more information on this issue and consider further revisions to the Principles as needed.

IV. REVISED PRINCIPLES

Based upon the staff's analysis of the comments discussing the Principles as initially proposed, and taking into account the key themes enumerated above, staff has revised the Principles. For purposes of clarification, the new language is set forth below in bold and italics. As noted above, these Principles are guidelines for self-regulation and do not affect the obligation of any company (whether or not covered by the Principles) to comply with all

---

[78] Where companies are using tracking data for non-behavioral advertising purposes, such uses may involve sharing the data with third parties. If so, the notice and choice that a company provides concerning such sharing may address at least some of the concerns raised about secondary uses. A secondary use may also constitute a retroactive "material change" to a company's existing privacy policy, in which case consumers could choose whether to provide affirmative express consent to the change.

applicable federal and state laws.

A. Definition

For purposes of the Principles, online behavioral advertising means the tracking of a consumer's online activities ***over time*** – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests. ***This definition is not intended to include "first party" advertising, where no data is shared with third parties, or contextual advertising, where an ad is based on a single visit to a web page or single search query.***

B. Principles

1. Transparency and Consumer Control

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option. ***Where the data collection occurs outside the traditional website context, companies should develop alternative methods of disclosure and consumer choice that meet the standards described above (i.e., clear, prominent, easy-to-use, etc.)***

2. Reasonable Security, and Limited Data Retention, for Consumer Data

Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the

nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company. ***Companies should also retain data only as long as is necessary to fulfill a legitimate business or law enforcement need.***

3. Affirmative Express Consent for Material Changes to Existing Privacy Promises

As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use ***previously collected*** data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising

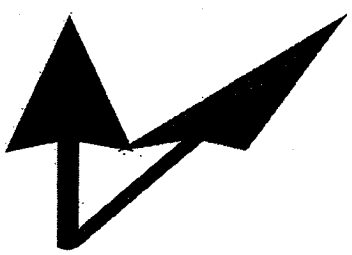
Companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

V. CONCLUSION

The revised Principles set forth in this Report constitute the next step in an ongoing process, and staff intends to continue the dialogue with all stakeholders in the behavioral advertising arena. Staff is encouraged by recent steps by certain industry members, but believes that significant work remains. Staff calls upon industry to redouble its efforts in developing self-regulatory programs, and also to ensure that any such programs include meaningful enforcement mechanisms. Self-regulation can work only if concerned industry members actively monitor compliance and ensure that violations have consequences.

Looking forward, the Commission will continue to monitor the marketplace closely so that it can take appropriate action to protect consumers. During the next year, Commission staff will evaluate the development of self-regulatory programs and the extent to which they serve the essential goals set out in the Principles; conduct investigations, where appropriate, of practices in the industry to determine if they violate Section 5 of the FTC Act or other laws; meet with companies, consumer groups, trade associations, and other stakeholders to keep pace with changes; and look for opportunities to use the Commission's research tools to study developments in this area.

The Commission is committed to protecting consumers' privacy and will continue to address the issues raised by online behavioral advertising.



SULLIVAN & CROMWELL LLP

TELEPHONE: 1-212-558-4000
FACSIMILE: 1-212-558-3588
WWW.SULLCROM.COM

125 Broad Street
New York, NY 10004-2498

LOS ANGELES • PALO ALTO • WASHINGTON, D.C.
FRANKFURT • LONDON • PARIS
BEIJING • HONG KONG • TOKYO
MELBOURNE • SYDNEY

January 29, 2009

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

Re: AT&T Inc. – Request to Exclude Stockholder Proposal of Trillium Asset Management Corp. on behalf of Jane Brown and Co-Proponents

Ladies and Gentlemen:

In our letter dated December 10, 2008, we asked the SEC Staff to concur in our view that AT&T Inc. ("AT&T" or the "Company") may omit the stockholder proposal (the "Proposal") submitted by Jonas Kron of Trillium Asset Management Corp. on behalf of Jane Brown and by other co-proponents from the proxy statement for the Company's 2009 annual meeting. In a letter dated January 9, 2009 (the "Reply Letter"), Mr. Kron asked the Staff not to grant the Company's request. On behalf of AT&T, we write to rebut Mr. Kron's principal arguments and to renew AT&T's request to omit the Proposal from its 2009 proxy statement in reliance on paragraphs (i)(7) and (i)(10) of Rule 14a-8, which permit exclusion of proposals that deal with ordinary business matters or have been substantially implemented.

Pursuant to Rule 14a-8(j), we enclose six paper copies of this letter and have also sent copies of this letter to Mr. Kron, Melissa Locke and Aditi Vora, the proponents' designated contacts.

Although the Reply Letter sets forth a great many assertions and references a lengthy list of news articles and other materials, we do not believe it is necessary to address all of these and instead will focus on the central arguments made in the letter. As described below, Mr. Kron's main point is that the Staff should reverse its longstanding

position under Rule 14a-8 that stockholder proposals dealing with customer privacy policies may be excluded because they deal with ordinary business matters. On this basis, Mr. Kron argues that the Staff should now require that the Proposal be included in the Company's 2009 proxy statement, even though it addresses substantially the same matters as the two earlier versions submitted by Mr. Kron, which the Staff previously concluded could be omitted from the Company's proxy statements in 2008 and 2007.

Mr. Kron also argues that AT&T needs to address privacy and free expression in a new public report, but he ignores the extensive public record that already sets forth AT&T's policies and views on these matters in considerable detail and provides no specifics about what, if anything, a new report would or could add to the public record. For this reason, we believe the Proposal has been substantially implemented and may also be excluded under paragraph (i)(10) of Rule 14a-8. For the same reason, we also believe there is considerable uncertainty as to what sort of report would satisfy the Proposal and the Reply Letter's great many assertions and references of questionable relevance to AT&T further underscore the Proposal's fundamentally vague, unfocused nature.

The Proposal Relates to Ordinary Business Matters and May Be Excluded Pursuant to Rule 14a-8(i)(7)

At its core, the Reply Letter asks the Staff to reverse its fundamental, longstanding and – in our view – correct position that stockholder proposals related to customer privacy policies may be excluded, arguing that "circumstances have changed such that [proposals dealing with customer privacy policies] should no longer be considered excludable". As we described in our initial letter, the Staff has long recognized that the protection of customer privacy is properly a management function that is not subject to stockholder oversight, and the Staff in many instances has allowed companies to exclude proposals requesting reports on issues related to customer privacy. See Letters regarding *Verizon Communications Inc.* (February 22, 2007); *Bank of America Corp.* (February 21, 2006); and *Applied Digital Solutions, Inc.* (March 25, 2006). The Reply Letter acknowledges that this has been the position of the Staff historically but argues that this year, at least with respect to the Proposal, this position is no longer valid and should be reversed.

The Reply Letter gives no reasoned explanation as to why customer privacy policies no longer involve ordinary business matters. The letter simply asserts that customer privacy policies should now be viewed as matters of "public policy" without offering any substantive reasons why the concerns that prompted the Staff to regard these matters as management functions in many recent decisions are no longer valid. In short, the Company's customer privacy policies still involve the same kinds of issues that the Staff has properly recognized are best addressed by management, not stockholders. Saying that they might implicate public policy in some circumstances with some audiences does not change the fact that they fundamentally involve ordinary business matters that are properly addressed by management.

Policies and procedures for handling customer information and the protection of customer privacy are essential to a company's day-to-day operations and, due to their complex and intricate nature – particularly in the context of AT&T's Internet network management practices that are the focus of the Proposal – these policies and procedures should be left to management oversight. As the Staff has appreciated in the past, the preparation of a report such as the one requested by the Proposal would unduly interfere with the Company's operations and create inefficiencies by shifting areas of day-to-day management responsibility to direct stockholder oversight. If the Staff were to reverse its longstanding position in this area, as the Reply Letter proposes, a highly complex management function, requiring difficult judgments about a number of technological, legal, business and operational considerations, would become subject to the vagaries of the proxy solicitation process. That would be an unfortunate result, subjecting to direct stockholder oversight matters that have traditionally and for good reason been left to management. At the very least, such a major change should not be undertaken without the proponents having shown good reasons why the important considerations underlying the Staff's established position are no longer valid.

The Reply Letter glosses over this core issue, stating that the Proposal focuses on "the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy". In essence, this is merely an assertion that customer privacy policies should be viewed as matters of public policy because the public has expressed interest in them. While the Reply Letter argues at great length that "[p]ublic expectations of privacy is [*sic*] clearly a significant policy issue", it ignores the fact that an analysis of Internet network management practices will inevitably focus on privacy considerations and thus relate to substantially the same subject matter that the Staff has found warranted exclusion of similar proposals from the Company's proxy materials in the past two years. See Letters regarding *AT&T Inc.* (February 9, 2007 and February 7, 2008).[1]

As noted in our initial letter, any evaluation of the Company's Internet network management practices would necessarily center around the concept of net neutrality. Such an evaluation would require a discussion of highly technical, fact-specific and complex matters such as "peering" and "deep packet inspection" – matters that the Reply Letter specifically cites. Yet matters such as these have long been viewed as the kinds that are appropriately addressed by management, not stockholders. For this reason, the Staff has previously concluded that stockholder proposals relating to net neutrality issues are excludable pursuant to Rule 14a-8(i)(7) on ordinary business

---

[1] The Reply Letter also asserts that "issues of public expectations of privacy . . . are no longer mundane matters" and that "the Internet has become more and more pervasive". There is no reason to believe that these assertions are any more meaningful now than they might have been in the past few years when the Staff permitted stockholder proposals in this area to be excluded. Yet even if they have somehow become more meaningful, they are beside the point, for they do not address the core issue – namely, that customer privacy policies are fundamentally matters best addressed by management. That has not changed.

grounds. See Letters regarding *Yahoo Inc.* (April 5, 2007) and *Microsoft Corporation* (September 29, 2006).

The Reply Letter also asserts that the Proposal does not focus on the Company's legal compliance program. Yet the topics of customer privacy and free expression on the Internet are inherently intertwined with legal and compliance issues, including issues relating to national security and law enforcement, and it is difficult to see how the Company could prepare the requested report without addressing these issues. They were the central focus of the proposals in the past two years, and merely omitting reference to them from this year's Proposal does not make them irrelevant. They are just as significant in 2009 as they were in 2008 and 2007. As noted in our initial letter, the Staff has long recognized that legal and compliance matters are management functions.

As we discussed in our initial letter, the Proposal is substantially the same as the two prior proposals, which the Staff permitted the Company to exclude from its proxy statements in 2008 and 2007. The Reply Letter tries to refute this key point by asserting that the Proposal differs from its predecessors in two important ways, but when examined closely these alleged differences are simply not meaningful in the context of Rule 14a-8. First, the Reply Letter emphasizes that the Proposal focuses not only on customer privacy but also on free expression.[2] With regard to either topic, however, the ultimate focus of the Proposal is on the Company's Internet network management practices, and there is no basis for concluding that these practices are any less intertwined with ordinary business matters when they implicate free expression than when they implicate customer privacy. In either case, the requested report would necessarily have to delve into a host of complex technical, legal, operational and business issues of the kind that have traditionally been viewed as the proper domain of management, not stockholders. Although it makes many references to the importance of free expression, the Reply Letter does not refute this basic point.

Second, the Reply Letter emphasizes that the Proposal focuses not on the Company's Internet network management practices relating to privacy and free expression, but on the *effects* that these practices have on these matters. This is a distinction without a difference. Whatever implications AT&T's management practices may have for customer privacy and free expression, the requested report would necessarily focus on the practices themselves. No purpose would be served by requiring the Company to prepare a lengthy report merely to provide extended commentary on the merits of privacy and free expression on the Internet. One cannot discuss the *effects* of Internet practices without discussing the practices themselves. Claiming that the Proposal differs from its predecessors because it focuses on the effects of these practices rather than the practices themselves is a meaningless distinction in this context. Like its predecessors, the Proposal would require a report that presents the kind of concrete,

---

[2] Although the Reply Letter discusses free expression at length, the proponents' supporting statement for the Proposal focuses exclusively on privacy concerns inherent in the "collecting and selling [of] personal information to third-parties". We think this fact is telling.

detailed issues that the Staff has repeatedly found are better left to management oversight.[3]

The Reply Letter concludes that "the [C]ompany bears the burden of persuasion" on excluding the Proposal from the 2009 proxy statement. We believe the Company has met this burden, by establishing that the Proposal relates to matters that the Staff has long recognized are ordinary business matters and are not the proper subject of stockholder proposals. The proponents have not offered any persuasive arguments to the contrary; rather, they argue that proposals addressing these matters should no longer be excludable. They urge the Staff to reverse its position in this area, and, in doing so, we believe they carry a greater burden of persuasion, which they have not met.

The Proposal Has Been Substantially Implemented and May Be Excluded Pursuant to Rule 14a-8(i)(10).

The Company recognizes that privacy and freedom of expression on the Internet are frequently discussed among lawmakers, regulators and the media. As we noted in our initial letter, AT&T has been a frequent participant in these discussions and has explained its evolving views on these topics in various public forums. For example, AT&T has already published and made numerous public statements about its policies regarding customer privacy, including those relating to Internet network management services. The Reply Letter does not dispute this point and instead asserts that these policies and statements do not address free expression. However, the Company has also published its policy on freedom of expression. For example, the AT&T High Speed Internet Terms of Service / att.net Terms of Use (which are available on the Internet at www.att.net) addresses freedom of expression.. Among other things, these terms state that "AT&T respects freedom of expression and believes it is a foundation of our free society to express differing points of view. AT&T Yahoo! will not terminate, disconnect or suspend service because of the views you or we express on public policy matters, political issues or political campaigns." As noted in our initial letter, the Company has also addressed freedom of expression in public hearings before federal regulators.

The Reply Letter cites two other reasons why the extensive public record does not address these topics in the way the proponents would prefer. First, it notes that the Proposal requests a report directed to AT&T stockholders, whereas the Company's many public statements on these matters have been directed toward a different audience (e.g., customers, regulators, lawmakers and the public at large). Yet the proponents offer no explanation as to why, in the context of issues that they allege involve "significant public policy concerns" and "public expectations of privacy and

---

[3] The Reply Letter refers to dozens of news articles and media presentations about the Internet without explaining how or even whether they relate to AT&T. What does definitely relate to AT&T, and what the requested report would have to focus on, is more down to earth: the Company's actual Internet network management practices. On the other hand, a report that instead focused on abstract, theoretical points in a public policy debate would be a piece of advocacy and would inject the Company into the political and legislative process. As the Reply Letter acknowledges, this would not be the proper subject for a stockholder proposal.

freedom of expression", the Company's many public statements on these topics are inadequate because they were not addressed solely to stockholders. Second, the Reply Letter notes that the Proposal requests a report prepared by the AT&T board, whereas the Company's public statements were made by members of management. This claim, however, overlooks the fact that the Company's published policies and public statements on these topics reflect the official views of AT&T, a corporation that is managed by its officers and employees who in turn are subject to the oversight and leadership of its board of directors.

By participating in numerous public discussions and publishing its policies as described above and in our initial letter, the Company has addressed the underlying concerns of the Proposal. We believe the Company has met the standard of "substantial implementation" that the Staff has previously articulated. See Letter regarding *Masco Corp.* (March 29, 1999); see also Letter regarding *Entergy, Inc.* (January 31, 2006). AT&T believes that the appropriate way to address these topics of public interest is to participate in the public debate about them, as it has done and expects to continue to do, and not to submit issues relating to the Company's ordinary business matters to the proxy solicitation process.

The Proposal Is Vague and Potentially Misleading and May Be Excluded Pursuant to Rule 14a-8(i)(3).

The Proposal requests a report about the Company's Internet management practices in the context of "the public's expectations of privacy and freedom of expression on the Internet". What, precisely, does this mean? Who is the "public" for this purpose and how is the Company to determine their collective "expectations"? These are matters for opinion pollsters and media commentators. The Company is not in a position to speculate about these matters and should not be required to do so. Any conclusions reached in the requested report in this regard would necessarily involve speculation, and would expose the Company to criticism and possibly even claims that it had failed to carry out the purposes of the Proposal.

The sprawling, open-ended nature of the Reply Letter, with its extensive list of media items and broad references to principles of free speech and privacy and to the importance of public policy and social issues, underscores the lack of concrete focus in the Proposal.[4] The Proposal provides very little guidance as to what is expected of the Company. The requested examination and report could proceed in many different directions, and there is no assurance that whichever path the Company chose would satisfy the proponents or stockholders generally.

The Proposal makes vague references to "significant policy concerns" and the "public's expectations of privacy and freedom of speech" without providing any indication as to the particular types of concerns and expectations that should be addressed in the

[4] It also underscores the fact that, in preparing any such report, the Company would have to focus – indeed, could only focus – on its actual day-to-day practices as opposed to various social or political issues that may be of interest to various segments of the public at large. In short, as discussed above, the requested report would have to focus on ordinary business matters, not public policy.

requested report. The Internet services provided by the Company are widely varied (including access to social networking sites, webcasts, email, e-commerce transactions, etc.) and are provided to many different segments of the public with significantly different expectations of privacy and free expression that depend in part on the context of the services they use. Furthermore, the Proposal's request that the report examine "Internet network management practices" does little to elucidate what aspects of these practices (whether technical, legal, commercial, operational or otherwise) should be addressed. Without clearer guidance, it is difficult to see how this Proposal, which is so sweeping in scope and encompasses so many varied and complex elements, can be implemented in a comprehensive yet efficient manner – or in any way that would meet the proponents' expectations.

Problems such as these have lead the Staff on many prior occasions to allow issuers, pursuant to Rule 14a-8(i)(3),to exclude stockholder proposals that contain overly general, unspecific or uninformative references to complex or varied sets of issues. See, e.g., Letters regarding *The Ryland Group, Inc.* (January 19, 2005); *Albertsons, Inc.* (March 5, 2004); and *Terex Corp.* (March 1,2004). We believe the Proposal may also be excluded on the ground that it is overly vague – that, if adopted by stockholders, the Company would not be able "to determine with any reasonable certainty exactly what actions or measures the proposal requires".[5]

Finally, it should be noted that the Proposal sets no limit on the amount of expense to be incurred by the Company in preparing and issuing the requested report. Consequently, the Proposal raises the same kinds of issues that the Staff has recognized as problematic in other contexts, where stockholder proposals purport to commit a company to making expenditures of corporate funds to achieve a stated goal without regard to whether the incurrence of those costs – or the stated goal itself – are in the best interests of all the stockholders or would result in a waste of corporate assets. The Company should not be required to prepare the requested report at more than a reasonable cost, as it may determine under the circumstances.

* * * * * * * * *

---

5 Staff Legal Bulletin No. 14B Section B.4. (September 15, 2004). See also Letters regarding *International Business Machines Corporation* (January 14, 1992); *FirstEnergy Corp.* (February 18, 2004); *Global Entertainment Holdings/Equities, Inc.* (July 10, 2003); *Pfizer Inc.* (February 18, 2003); and *Johnson & Johnson* (February 7,2003).