

NO ACT

PC  
12-2208



DIVISION OF  
CORPORATION FINANCE

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



09004147

Received SEC  
FEB 13 2009  
Washington, DC 20549

February 13, 2009

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

Act: 1934  
Section: \_\_\_\_\_  
Rule: 14a-8  
Public  
Availability: 2-13-09

Re: Verizon Communications Inc.  
Incoming letter dated December 22, 2008

Dear Ms. Weber:

This is in response to your letters dated December 22, 2008 and January 27, 2009 concerning the shareholder proposal submitted to Verizon by Paul Haible and Trillium Asset Management Corporation. We also received on behalf of the proponents a letter on January 20, 2009 and two letters on February 12, 2009. Our response is attached to the enclosed photocopy of your correspondence. By doing this, we avoid having to recite or summarize the facts set forth in the correspondence. Copies of all of the correspondence also will be provided to the proponents.

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

Sincerely,

PROCESSED  
MAR 02 2009  
THOMSON REUTERS

Heather L. Maples  
Senior Special Counsel

Enclosures

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

February 13, 2009

**Response of the Office of Chief Counsel  
Division of Corporation Finance**

Re: Verizon Communications Inc.  
Incoming letter dated December 22, 2008

The proposal requests the board to issue a report examining the effects of Verizon's internet network management practices.

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

Sincerely,

Philip Rothenberg  
Attorney-Adviser

**DIVISION OF CORPORATION FINANCE  
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS**

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

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

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

February 12, 2009

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 Verizon Communications Inc. for 2009 Proxy Statement

Dear Sir/Madam:

This letter is submitted on behalf of Paul Heible, Richard Ames, and Trillium Asset Management Corporation (hereinafter referred to as "Proponents"), who are beneficial owners of shares of common stock of Verizon Communications Inc. (hereinafter referred to as "Verizon" or the "Company"), and is a response to Verizon's ("the Company") second letter on this matter, dated January 27, 2009. A copy of this letter is being e-mailed concurrently to Verizon's Assistant General Counsel Mary Louise Weber at [mary.l.weber@verizon.com](mailto:mary.l.weber@verizon.com).

While the Company letter, which is as long as its original letter, seeks to re-argue all of its original contentions we stand firmly by our January 20, 2009 letter and incorporate it herein. Because of the repetitive nature of many of the Company's assertions it is not necessary to respond to each and every point raised in the Company's protracted January 27<sup>th</sup> letter. However, mindful of the large number of no-action letter requests the Staff is now considering and the need for conciseness, we would respectfully like to address the Company's latest assertions as briefly as possible.

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. This issue was the subject of a November 30<sup>th</sup> 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...

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

1. The Proposal seeks to micro-manage the Company or does not focus on a significant public policy issue;
2. Verizon has substantially implemented the Proposal; or
3. The Proposal is so vague that it would be impossible to implement.

BOSTON	DURHAM	SAN FRANCISCO	BOISE
711 Atlantic Avenue Boston, Massachusetts 02111-2809 T: 617-423-6655 F: 617-482-6179 800-548-5684	353 West Main Street, Second Floor Durham, North Carolina 27701-3215 T: 919-688-1265 F: 919-688-1451 800-853-1311	369 Pine Street, Suite 711 San Francisco, California 94104-3310 T: 415-392-4806 F: 415-392-4535 800-933-4806	950 W. Bannock Street, Suite 530 Boise, Idaho 83702-6118 T: 208-387-0777 F: 208-387-0278 800-567-0536

## **The Proposal**

For the Staff's convenience, the Proposal's resolved clause is as follows:

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.

### **The Company has not met its burden of proving that the Proposal can be excluded under Rule 14a-8(i)(7).**

In spite of all the debate over the ordinary business rule, we believe that the analysis required by Rule 14a-8(i)(7) is in fact quite simple. It begins with the fundamental understanding that "all proposals could be seen as involving some aspect of day-to-day business operations." *Amalgamated Clothing and Textile Workers Union v. Wal-Mart Stores, Inc.*, 821 F. Supp. 877, 891 (S.D.N.Y. 1993). Therefore, "proposals relating to such [day-to-day] matters but focusing on sufficiently significant social policy issues ... generally would not be considered to be excludable." Exchange Act Release No. 34-40018 (May 21, 1998) ("1998 Interpretive Release"). However, if a "proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment" it can be excluded. *Id.*

We will concede that to the extent that all proposals involve some aspect of day-to-day operations, that the Proposal does as well. What is critical, however, is whether the Proposal also focuses on a significant social policy issue without seeking to micro-manage the company. If it does, or more accurately if the Company fails to prove that it does not, then it must appear in the company's proxy materials.

Looking at the first question – significant social policy issue – we think it is abundantly clear that the Proposal does just that. As evidence that it focuses on a significant policy issue we cite in our January 20<sup>th</sup> letter to Verizon's own Congressional testimony; over 50 specific, original and detailed stories in major national publications; federal regulatory inquiries and actions; Congressional hearings; and public polling data. We also note here that under the terms of House Resolution 31, unanimously adopted by the House of Representatives, January 28<sup>th</sup> was declared National Data Privacy Day in the United States. This significant body of evidence of a widespread public debate, not only on public expectations of privacy but also on freedom of expression issues, goes far beyond the requirements of the Rule. And 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.

Turning to the second issue – micro-management – it is clear that we are not seeking "intricate detail, or seeks specific time-frames or methods for implementing complex policies." 1998 Interpretive Release. The plain language of the Proposal demonstrates that we are not seeking disclosure of the intricate details of network management policies or practices – the Proposal focuses on the impact of the Company on society. Neither are we seeking to impose any methods for implementing complex network management policies – again the Proposal focuses on impacts, not policies. And there is certainly no mention of specific time frames in the Proposal. This formulation of the proposal, focusing on the impact of the company on society fits clearly within the model presented by Staff Legal Bulletin No. 14C. Finally, in neither letter does the Company assert a micro-management argument. As with the significant social policy issue, we believe the Company has not met its burden of proof on this point.

Rather than re-argue every point the Company already made in its second letter, we respectfully refer the Staff to our January 20<sup>th</sup> letter. Freedom of expression and public expectations of privacy are of fundamental strategic importance to Verizon, its shareholders and our society. The change presented

by the Internet challenges basic understandings of our most fundamental societal values and the role our Company plays in this changing landscape. Our Proposal seeks to focus the Board's strategic vision on critical issues, not on the mundane matters regarding the precise wording of privacy policies, or the paperwork required to release a credit card number, or the nuances of intellectual property law, for example. Freedom of speech and public expectations of privacy are the very "fundamental business strategy" issues and "long term goals" that the Rule is intended to bring before shareholders. *Roosevelt v. E.I. DuPont de Nemours & Co.*, 958 F. 2d 416 (DC Cir. 1992). Therefore, in the interests of shareholder rights, our Constitutional form of government, and the vitality of our society, we respectfully ask the Staff to reject the Company's arguments.

**The Proposal has not been substantially implemented nor is it vague.**

The Company has not introduced any new arguments with respect to substantial implementation and we do not want to occupy the Staff's time duplicating the arguments we made in our January 20<sup>th</sup> letter. We recognize that these kinds of arguments are very fact intensive and therefore refer the Staff to the details in our previous letter. Suffice it to say, that the Company does not challenge the factual premise of our argument and it is undisputed that the policies:

- do not constitute an examination of freedom of speech and privacy issues;
- are not the result of a Board examination of these issues;
- are not presented in a single document; and
- are not prepared for a shareholder audience

Each of these facts are substantial and relevant as found by the Staff in *Newell Rubbermaid Inc.* (February 21, 2001); *PPG Industries, Inc.* (January 22, 2001); *NYNEX Corporation* (February 16, 1994); *NYNEX Corporation* (February 18, 1994); *Associates First Capital Corporation* (March 13, 2000); and *Wendy's International* (February 21, 2006).

As discussed in our January 20<sup>th</sup> letter, vagueness determinations can become very fact-intensive determination and the Staff has expressed concern about becoming overly involved in such determinations. Staff Legal Bulletin No. 14B (September 15, 2004). We stand firmly by our analysis in our January 20<sup>th</sup> letter and suggest that the Company has underestimated the ability of its shareholders to understand the plain meaning of the Proposal. Leaving aside all of the Company's rhetoric, if one simply reads the Proposal it is clear that the Company has not met its burden of demonstrating the Proposal is "so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." *Id.* We have also taken the step in the Supporting Statement, within the significant length restrictions imposed by the Rule, of providing shareholders and the Board with some illustrative guidance as to the issues the Board could address. We are asking for an examination of 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 – nothing more, nothing less. Despite vigorous attempts to plant seeds of confusion, Verizon has not demonstrated how this is inherently vague or indefinite. As a plain reading of the Proposal demonstrates, it raises the subject of public expectations of privacy rights and freedom of expression clearly and succinctly.

We suspect the Company is trying to portray the Proposal as an academic exercise. We believe, however, the Company has not demonstrated it is adequately addressing the issues of public expectations of privacy and freedom of expression. This Proposal is an opportunity for shareholders to express their concurrence or disagreement with this conclusion. We are suggesting the Board address it as a report to address how the company effects public expectations of privacy and freedom of speech.<sup>1</sup>

<sup>1</sup> We are gratified to observe that the Company has apparently dropped its "false and misleading" arguments and have heeded the disfavor expressed by the Staff.

Finally, we reiterate that the Company cannot argue the point both ways – either the Company has implemented the Proposal or it is too vague to be able to implement, but it cannot be both. Therefore, we respectfully request the Staff reject the Company's argument on both points.

**There is no serious dispute that Trillium is in fact a co-filer and that ownership and authorization were properly documented.**

With respect to the ownership and authorization issues, it would appear that there is a factual dispute as to what we sent to the Company on November 26, 2008. We vehemently assert that we sent all the necessary documents to the Company on that date, the Company apparently disagrees. We have provided evidence to substantiate our position in our first letter and the Company has simply asserted a contrary position. We would suggest that the Staff is not intended to be an arbiter of factual disputes and therefore should not concur with the Company.

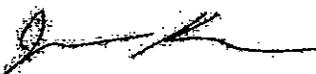
As for the co-filing question, all the evidence, not the least of which is Trillium's acting on behalf of Mr. Haible before the Staff, indicates that Mr. Ames and Trillium are co-filing this Proposal. To conclude otherwise is contrary to the obvious. We would note that a reasonable way to address this situation can be found with a similar question raised by Comcast in its January 15, 2009 amended no-action request. In that case the simple clarification provided by the co-filer was sufficient for the company to end its questioning of the co-filer's status and allow the Staff to focus on the material questions presented by the no-action request. We respectfully contend that argument of this nature only serves to distract and waste the Staff's time.

#### **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](mailto: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](mailto:jkron@trilliuminvest.com).

Sincerely,



Jonas Kron,  
Senior Social Research Analyst

Enclosures

cc: John Harrington, Harrington Investments

Paul Haible

Richard Ames

February 12, 2009

VIA e-mail: [shareholderproposals@sec.gov](mailto: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 Verizon Communications Inc. for 2009 Proxy Statement

Dear Sir/Madam:

This letter is submitted on behalf of Paul Heible, Richard Ames, and Trillium Asset Management Corporation (hereinafter referred to as "Proponents"), who are beneficial owners of shares of common stock of Verizon Communications Inc. (hereinafter referred to as "Verizon" or the "Company"), and is a response to Verizon's ("the Company") second letter on this matter, dated January 27, 2009. A copy of this letter is being e-mailed concurrently to Verizon's Assistant General Counsel Mary Louise Weber at [mary.l.weber@verizon.com](mailto:mary.l.weber@verizon.com).

After we filed our reply to Verizon's January 27, 2008 letter earlier today, the Federal Trade Commission ("FTC") issued a report entitled "Self-Regulatory Principles For Online Behavioral Advertising" which focuses on privacy concerns. Specifically, the Report observes that "the ease with which companies can collect and combine information from consumers online has raised questions and concerns about consumer privacy." The Report goes on to express concern about the numerous threats to Internet users' privacy. See attached copy of Report.

The Report discussed a number of recent developments in the area of privacy, many of which we raised in our January 20, 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 Verizon 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.

**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

After that discussion, the Report concluded that:

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). Accordingly, the FTC announced its revised Self-Regulatory Principles For Online Behavioral Advertising .

We urge the Staff to consider seriously the conclusions of its sister agency and recognize that Internet privacy is a significant public policy issue that transcend the day-to-day affairs of the Company. We are in a society, political environment and economy that is grappling with the new challenges the Internet poses to our civil liberties. We believe the Board must address these concerns in a strategic manner for the good of our society and the financial well-being of the Company. These issues are of significant public interest and therefore it is appropriate under Rule 14a-8 for shareholders to consider our Proposal in our Company's proxy materials.

Please contact me at (971) 222-3366 or [jkron@trilliuminvest.com](mailto: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](mailto:jkron@trilliuminvest.com).

Sincerely,



Jonas Kron,  
Senior Social Research Analyst

Enclosures

cc: John Harrington, Harrington Investments

Paul Haible

Richard Ames

**FTC Staff Report:**  
**Self-Regulatory Principles**  
**For Online Behavioral Advertising**



**Behavioral Advertising**  
**Tracking, Targeting, & Technology**

*February 2009*

## TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	i
I. INTRODUCTION.....	1
II. BACKGROUND.....	2
A. What Is Online Behavioral Advertising?.....	2
B. The FTC's Examination of Online Behavioral Advertising.....	4
1. Online Profiling Workshop.....	6
2. Tech-ade Hearings and the Behavioral Advertising Town Hall.....	8
C. Staff's Proposed Self-Regulatory Principles.....	11
D. Recent Initiatives to Address Privacy Concerns.....	12
III. SUMMARY OF THE COMMENTS RECEIVED AND STAFF'S ANALYSIS.....	18
A. The Principles' Scope.....	20
1. Applicability to Non-PII.....	20
2. Applicability to "First Party" Online Behavioral Advertising.....	26
3. Applicability to Contextual Advertising.....	29
B. Transparency and Consumer Control.....	30
1. Choice for Non-PII.....	31
2. Providing Effective Notice and Choice.....	33
C. Reasonable Security and Limited Data Retention for Consumer Data.....	37
D. Affirmative Express Consent for Material Retroactive Changes to Privacy Promises.....	39
E. Affirmative Express Consent to (or Prohibition Against) Use of Sensitive Data.....	42
F. Secondary Uses.....	44
IV. REVISED PRINCIPLES.....	45
A. Definition.....	46
B. Principles.....	46
1. Transparency and Consumer Control.....	46
2. Reasonable Security, and Limited Data Retention, for Consumer Data.....	46
3. Affirmative Express Consent for Material Changes to Existing Privacy Promises.....	47
4. Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising.....	47
V. CONCLUSION.....	47

**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.<sup>1</sup> 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.<sup>2</sup> 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

---

<sup>1</sup> 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>.

<sup>2</sup> 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"<sup>3</sup> to track consumers' activities and associate those activities with a particular computer or device.<sup>4</sup> Many of the companies engaged in behavioral advertising are so-called

---

<sup>3</sup> 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."

<sup>4</sup> 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.<sup>5</sup>

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

---

<sup>5</sup> 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."<sup>6</sup> 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.<sup>7</sup> In addition to these

---

<sup>6</sup> 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.

<sup>7</sup> 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.<sup>8</sup>

---

*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.shtml>; 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.shtml>; 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.shtml>; 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.shtml>; 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.shtml>.

<sup>8</sup> 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.<sup>9</sup> 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.<sup>10</sup> 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).

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

<sup>10</sup> 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”),<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup>

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.<sup>14</sup>

---

<sup>11</sup> July 2000 Report, available at <http://www.ftc.gov/os/2000/07/onlineprofiling.pdf>.

<sup>12</sup> 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.

<sup>13</sup> See July 2000 Report, *supra* note 11, at 10-11.

<sup>14</sup> 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 Behavioral 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.<sup>15</sup> 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,<sup>16</sup> 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.<sup>17</sup>

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.<sup>18</sup> Further, the announcement

---

<sup>15</sup> *Id.* See also Ryan Blitstein, *Microsoft, Google, Yahoo in Online Ad War*, SAN JOSE MERCURY NEWS, May 19, 2007.

<sup>16</sup> 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>.

<sup>17</sup> 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](http://www.ftc.gov/bcp/workshops/techade/pdfs/transcript_061107.pdf) (panel discussion entitled "Marketing and Advertising in the Next Tech-ade").

<sup>18</sup> 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.<sup>19</sup> 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.<sup>20</sup> Based on the discussion, several core principles emerged. First, as discussed above, online behavioral advertising<sup>21</sup> may provide valuable

---

<sup>19</sup> 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>.

<sup>20</sup> 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>.

<sup>21</sup> 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.<sup>22</sup>

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.<sup>23</sup> Further, while various industry associations discussed their online self-regulatory schemes to address privacy issues, these schemes did not generally focus on behavioral advertising.<sup>24</sup>

---

<sup>22</sup> 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>.

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

<sup>24</sup> *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.<sup>25</sup> 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.<sup>26</sup> 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.<sup>27</sup> In particular, both Google and Yahoo! Inc. ("Yahoo!") have announced new tools that will allow consumers to opt out of receiving targeted online advertisements.<sup>28</sup> Microsoft Corporation has announced that the new version of

---

<sup>25</sup> 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.

<sup>26</sup> 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.

<sup>27</sup> 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.

<sup>28</sup> 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.<sup>29</sup> Other steps include educational programs to inform consumers about online tracking<sup>30</sup> and new policies to reduce the length of time companies store personal data collected about online searches.<sup>31</sup>

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").<sup>32</sup> 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).

<sup>29</sup> See Gregg Keizer, *Microsoft Adds Privacy Tools to IE8*, COMPUTERWORLD.COM, Aug. 25, 2008, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=91134> 19. 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.

<sup>30</sup> 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\\_playlist?p=ECB20E29232BCBBA](http://www.youtube.com/view_playlist?p=ECB20E29232BCBBA) (last visited Jan. 9, 2009).

<sup>31</sup> See Posting of Kim Hart, [washingtonpost.com](http://voices.washingtonpost.com/posttech/2008/12/yahoo_changes_data-retention_p.html?nav=rss_blog), to [http://voices.washingtonpost.com/posttech/2008/12/yahoo\\_changes\\_data-retention\\_p.html?nav=rss\\_blog](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).

<sup>32</sup> See NAI, *2008 NAI Principles Code of Conduct* (Dec. 16, 2008), available at [http://www.networkadvertising.org/networks/2008%20NAI%20Principles\\_final%20for%20Web\\_site.pdf](http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Web_site.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.<sup>33</sup> 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.<sup>34</sup>

---

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](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.

<sup>33</sup> 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.

<sup>34</sup> 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.<sup>35</sup> 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.<sup>36</sup> 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.<sup>37</sup>

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](http://www.iab.net/iab_products_and_industry_services/1421/1443/1464).

<sup>35</sup> 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>.

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

<sup>37</sup> See TRUSTe, *Online Behavioral Advertising: A Checklist of Practices that Impact Consumer Trust*, available at [http://www.truste.com/about/online\\_behavioral\\_advertising.php](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.<sup>38</sup> Witnesses from the FTC,<sup>39</sup> 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”).<sup>40</sup> 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.

---

<sup>38</sup> *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](http://commerce.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=e46b0d9f-562e-41a6-b460-a714bf37017).

<sup>39</sup> See *id.* (statement of Lydia Parnes, Director of the FTC Bureau of Consumer Protection).

<sup>40</sup> *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](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.<sup>41</sup> 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.<sup>42</sup> The companies' responses are available online.<sup>43</sup>

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.

---

<sup>41</sup> *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](http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml).

<sup>42</sup> 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](http://energycommerce.house.gov/Press_110/110-ltr.080108.AOL-TILetters.pdf).

<sup>43</sup> 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](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.<sup>44</sup> 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

---

<sup>44</sup> 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.<sup>45</sup> 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.<sup>46</sup> 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

---

<sup>45</sup> See *supra* note 8 (citing FTC settlements requiring companies to implement reasonable information security programs to protect sensitive personal information).

<sup>46</sup> 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");<sup>47</sup> 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

---

<sup>47</sup> 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,<sup>48</sup> 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

---

<sup>48</sup> 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,<sup>49</sup> 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.<sup>50</sup>

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

---

<sup>49</sup> 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).

<sup>50</sup> 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.<sup>51</sup>

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

---

<sup>51</sup> 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](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.<sup>52</sup> 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.<sup>53</sup>

---

<sup>52</sup> 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](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](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](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, *Behavioral 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, *Behavioral 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).

<sup>53</sup> 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.<sup>54</sup> 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\\_12\\_13](http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_12_13) (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).

<sup>54</sup> 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.<sup>55</sup>

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

---

<sup>55</sup> 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.<sup>56</sup> 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.<sup>57</sup> If a website collects and then sells or shares data with third parties for purposes of behavioral advertising,<sup>58</sup> 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.<sup>59</sup>

---

<sup>56</sup> 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 Association (“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).

<sup>57</sup> 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.

<sup>58</sup> 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.

<sup>59</sup> 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.<sup>60</sup> 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

---

<sup>60</sup> 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.<sup>61</sup> 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.<sup>62</sup>

---

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

<sup>62</sup> 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<sup>63</sup> 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.<sup>64</sup> 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.

<sup>63</sup> 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.

<sup>64</sup> 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<sup>65</sup> 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

---

<sup>65</sup> 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.<sup>66</sup> 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.<sup>67</sup> 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

---

<sup>66</sup> 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.

<sup>67</sup> *See, e.g.*, Jon Leibowitz, Commissioner, FTC, Remarks at the FTC Town Hall Meeting on "Behavioral Advertising: Tracking, Targeting, & Technology" at 4-5 (Nov. 1, 2007), available at <http://www.ftc.gov/speeches/leibowitz/071031behavior.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.<sup>68</sup> Staff therefore encourages stakeholders to

---

<sup>68</sup> 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,<sup>69</sup> 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

---

<sup>69</sup> 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.<sup>70</sup>

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.<sup>71</sup> 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.<sup>72</sup> 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

---

<sup>70</sup> 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).

<sup>71</sup> *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).

<sup>72</sup> *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*<sup>73</sup> 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.<sup>74</sup>

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

---

<sup>73</sup> 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.

<sup>74</sup> 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.<sup>75</sup>

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,

---

<sup>75</sup> 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](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<sup>76</sup> 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.<sup>76</sup> 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

---

<sup>76</sup> 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.<sup>77</sup> 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

---

<sup>77</sup> 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.<sup>78</sup> 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

---

<sup>78</sup> 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

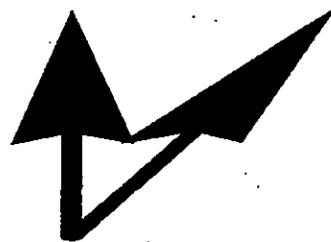
Companies should collect sensitive data for behavioral advertising only after they obtain affirmative express consent from the consumer to receive such advertising.

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.



---

**Federal Trade Commission**  
**ftc.gov**

Mary Louise Weber  
Assistant General Counsel



One Verizon Way, Rm VC54S440  
Basking Ridge, NJ 07920  
Tel 908 559-5636  
Fax 908 696-2068  
mary.l.weber@verizon.com

January 27, 2009

**By email to 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: Verizon Communications Inc. 2009 Annual Meeting  
Supplement to Letter Dated December 22, 2008  
Related to the Shareholder Proposals of Paul Haible  
and Trillium Asset Management Corporation

Ladies and Gentlemen:

I refer to my letter dated December 22, 2008 (the "December 22 Letter") pursuant to which Verizon Communications Inc., a Delaware corporation ("Verizon"), requested that the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission (the "Commission") concur with Verizon's view that (i) the shareholder proposal and supporting statement (the "Haible Proposal") submitted by Paul Haible ("Mr. Haible") and the shareholder proposal and supporting statement (the "Trillium Proposal") submitted by Trillium Asset Management Corporation ("Trillium"), on behalf of certain of its clients, may be properly omitted pursuant to Rule 14a-8(i)(10), Rule 14a-8(i)(7), Rule 14a-8(i)(3) and Rule 14a-8(i)(6) from the proxy materials to be distributed by Verizon in connection with its 2009 annual meeting of shareholders ("the 2009 proxy materials"), and (ii) the Trillium Proposal also may be properly omitted pursuant to Rule 14a-8(f). In addition, as stated in the December 22 Letter, if the Staff is unable to agree that the Haible Proposal may be omitted from the 2009 proxy materials, Verizon requests that the Staff concur with Verizon's view that the Trillium Proposal may be properly omitted pursuant to Rule 14a-8(i)(11). The Trillium Proposal and the Haible Proposal are sometimes collectively referred to herein as the "Proposal" and Trillium and Mr. Haible are sometimes collectively referred to herein as the "Proponents."

This letter is in response to the letter to the Staff dated January 20, 2009<sup>1</sup> (the "Proponents' Response Letter") submitted by Trillium, on behalf of itself, Mr. Haible and Richard Ames ("Mr. Ames"), and supplements the December 22 Letter. Mr. Ames has authorized Trillium to represent him with respect to the Proposal.

In accordance with Staff Legal Bulletin No. 14D (November 7, 2008), this letter is being emailed to [shareholderproposals@sec.gov](mailto:shareholderproposals@sec.gov). A copy of this letter is being sent by overnight courier to Trillium, Mr. Haible and Mr. Ames.

#### I. Introduction.

The purpose of Rule 14a-8 is to provide "an avenue for communication between shareholders and companies, as well as among shareholders themselves." Staff Legal Bulletin No. 14, Section B.1. (July 13, 2001) ("SLB No. 14"). Implicit in this is that the subject of the communication be a topic relating to the company, its business and its shareholders (subject to the enumerated bases for exclusion under Rule 14a-8). Here, the Proponents' Response Letter makes it entirely clear that the Proponents are seeking to engage Verizon in a wide-ranging, academic "examination" and "exploration" of issues that, while undoubtedly of interest to the Proponents, have little bearing on Verizon's business or the interests of Verizon's shareholders. For example, the Proponents' Response Letter states:

- "The Proponents have requested an *examination* of free speech and privacy issues and that implicitly calls for a presentation of differing ideas and approaches" (page 4) (emphasis in original);
- The requested report "does not ask for a specific result or policy" (page 4);
- The requested report should be an "exploration of the impact the company has on our national values of privacy and free speech" (page 4); and
- "We are intending this report to be an examination of how the Company has an impact on our society and how privacy interests are impacted by commercial interests" (page 18).

These statements and others in the Proponents' Response Letter demonstrate an agenda of interest to the Proponents, and the Proponents' Response Letter reads, in large part, more like a graduate student's doctoral thesis or a government "white paper" than a Rule 14a-8 argument supporting inclusion of a proposal in a company's proxy materials. The Proponents seek to engage Verizon in a philosophical debate on "differing ideas and approaches" to "our national values of privacy and free speech." This, we believe, is not a proper use of the Rule 14a-8 process.

---

<sup>1</sup> The Proponents' Response Letter was erroneously dated January 20, 2008.

**II. Verizon's Response to the Proponents' Response Letter.**

**A. The Proponents Improperly Apply Rule 14a-8(i)(10) by Asserting that Substantial Implementation Requires a Company to Comply with Non-Essential Aspects of a Proposal.**

As discussed in Section II.A. of the December 22 Letter, a company need not comply with every aspect of a proposal so long as the company's actions satisfactorily address the proposal's underlying concerns. Indeed, the Proponents' Response Letter, on page 5, readily acknowledges that Verizon is correct in its argument that in order for Rule 14a-8(i)(10) to apply, a company is "required to 'substantially implement' proposals *rather than 'fully implement' proposals*" (emphasis added). Nevertheless, the Proponents' Response Letter argues that Verizon has failed to satisfy Rule 14a-8(i)(10) because it has not complied with certain aspects of the Proposal which are not essential to the Proposal's underlying concern.

Section II.A. of the December 22 Letter describes Verizon's relevant policies and principles relating to free speech and privacy posted on its website. The Proponents' Response Letter, however, claims on page 4 that such information does not constitute an "examination of freedom of speech and privacy issues" which "implicitly calls for a presentation of differing ideas and approaches," and that the information Verizon has provided does not "rise to the level of a discussion or exploration of the impact the company has on our national values of privacy and free speech." Nothing in the Proposal requires the requested report to present "differing ideas and approaches" on freedom of speech and privacy. This after-the-fact argument appears to be an ill-conceived attempt to justify the Proponents' assertion that Verizon has not substantially implemented the Proposal.

In addition, the Proponents' Response Letter argues, on page 4, that Verizon has not substantially implemented the Proposal because Verizon does not "present the information in the same form as we request." This argument is without merit. "Substantial implementation" does not require a company to present information in the "same form" as a proponent requests. Verizon has posted the relevant information on its website and made this information publicly available to its shareholders and other interested parties. The Proponents have not shown that shareholders are prejudiced by having access to information over the website as opposed to having access to information through the requested report. Furthermore, to the extent the Proponents object to the fact that information has been presented in the form of policies and company statements rather than a single report, the Staff has consistently taken the position that shareholder proposals have been substantially implemented when a company already has policies and procedures in place relating to the subject matter of the proposal, despite the fact that the proposal requested a "report." *See, e.g., The Gap, Inc.* (March 16, 2001) (permitting exclusion of a proposal requesting a report on child labor practices of the company's suppliers as substantially implemented, where

the company had adopted a code of vendor conduct, monitored vendor compliance and published related information on its website); *Honeywell International, Inc.* (February 21, 2006) (permitting exclusion of a proposal requesting a sustainability report as substantially implemented, despite proponent's objection that the report proffered by the company was insufficient because it was no more than "a sketchy marketing presentation, with little or no data or analysis").

In a similar vein, the Proponents' Response Letter, on page 4, contends that Verizon has not substantially implemented the Proposal because the website information "is intended to communicate information to *customers*, while the Proposal requests information for *shareholders*" (emphasis in original). As discussed above, the website information is publicly available and therefore equally available to customers and shareholders alike. The Proponents fail to demonstrate how this constitutes an essential element of the Proposal such that Verizon is precluded from relying on Rule 14a-8(i)(10) as a basis to exclude the Proposal.

The Proponents' Response Letter, on page 4, also claims that Verizon's "policies and statements are not the product of a *board examination*" (emphasis in original). For purposes of this objection, the Proponents have recast the primary focus of the Proposal as a "board examination," rather than a report on free speech and privacy issues, and argue, on page 5 of the Proponents' Response Letter, that "employee/management level activities are not a substitute" for board examination. Although the Proponents offer several precedents in support of their assertion, the precedents are entirely distinguishable from the Proposal. In the cited letters, each of the proposals specifically requested that the board create a committee and therefore board or board committee participation was an explicit and essential component of the proposal. For example, in *NYNEX Corporation* (February 16, 1994), which the Proponents' Response Letter cites on pages 4-5, the proposal requested that the company establish a four-member committee of its board to evaluate the impact of various health care proposals on the company and to prepare a report. The other letters cited by the Proponents likewise relate to proposals requesting the creation of a board committee. In contrast, the Proposal does not request that Verizon create a board committee charged with the responsibility of evaluating a particular subject; the Proposal simply requests that "the board issue a report." Accordingly, the Proponents' assertions fail to refute Verizon's argument that the Proposal has been substantially implemented and is therefore excludable on the basis of Rule 14a-8(i)(10).

**B. The Proponents Incorrectly Argue that the Mere Presence of a Significant Social Policy Issue Precludes a Company from Relying on Rule 14a-8(i)(7).**

The Proponents incorrectly argue that the mere presence of a significant social policy issue precludes a company from relying on the ordinary business exclusion under Rule 14a-8(i)(7). However, the Proponents' interpretation of Rule 14a-8(i)(7) fails

to address the numerous precedents in which the Staff has concurred in the exclusion of proposals on ordinary business grounds, even where such proposals touched on significant social policy issues. The determination as to whether exclusion pursuant to Rule 14a-8(i)(7) is proper is not whether a significant social policy issue may be present in a proposal, but whether and to what extent such policy issue constitutes the focus of the proposal.

The Proponents' Response Letter flatly asserts, on page 5, that a proposal cannot be excluded under Rule 14a-8(i)(7) "if it has 'significant policy, economic or other implications,'" quoting *Roosevelt v. E.I. Du Pont de Nemours & Co.* in support of its claim. However, the *DuPont* case does not stand for the proposition, as asserted by the Proponent, that the implication of a significant policy issue will remove a proposal from the reach of Rule 14a-8(i)(7). In *DuPont*, which involved a shareholder proposal related to the effects of chlorofluorocarbons ("CFC") on the ozone and requested that the company rapidly accelerate its plans to phase out CFC production, the court acknowledged that despite the clear public interest in the topic, a determination of whether the proposal implicated ordinary business was related to the degree to which the ordinary business matter dominated the proposal:

We recognize that "ordinary business operations" ordinarily do not attract the interest of both the executive and legislative branches of the federal government. ... But government regulation of the CFC phase out, even the President's headline-attracting decision to accelerate the schedule initially set by Congress, does not automatically elevate shareholder proposals on timing to the status of "significant policy." What the President and Congress have said about CFCs is not the subject of our closest look. Instead, Rule 14a-8(c)(7) [predecessor to Rule 14a-8(i)(7)] requires us to home in on [the shareholder's] proposal, to determine whether her request *dominantly implicates ordinary business matters*. *Roosevelt v. E.I. Du Pont de Nemours & Co.*, 958 F.2d 416, 428 (D.C. Cir. 1992) (emphasis added).

Here, although the Proponents make several sweeping references to human rights, social policy and social goods throughout the Proponents' Response Letter in an effort to tie the Proposal to significant policy considerations, the dominant and clear thrust of the Proposal is on ordinary business matters, namely, the procedures and practices for protecting customer information.

Even if the Proposal is deemed to implicate a significant social policy issue, it is clear that the presence of a significant social policy issue will not undermine exclusion under Rule 14a-8(i)(7). As discussed in Section II.B.2. of the December 22 Letter, the cited precedents demonstrate that the applicability of Rule 14a-8(i)(7) depends largely on whether the 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. The Staff has in numerous instances permitted exclusion of proposals in which the proposals related to a company's ordinary business operations also involved a significant social policy issue.

For example, in *General Electric Co.* (February 3, 2005), the Staff permitted exclusion of a proposal relating to the elimination of jobs within the company and/or the relocation of U.S.-based jobs by the company to foreign countries pursuant to Rule 14a-8(i)(7) because it related to "management of the workforce," despite the proponent's objection that "the thrust and focus of [the] proposal is not on an ordinary business matter, but on the significant social policy issue of outsourcing jobs." In *Chrysler Corp.* (February 18, 1998), the Staff permitted exclusion of a proposal that dealt with matters both within and outside the scope of ordinary business and noted:

[A]lthough the balance of the proposal and supporting statement appears to address matters outside the scope of ordinary business, paragraph 5 of the resolution relates to ordinary business matters, and paragraph 6 is susceptible to a variety of interpretations, some of which could involve ordinary business matters. Accordingly, insofar as it has not been the Division's practice to permit revisions under rule 14a-8(c)(7), we will not recommend enforcement action to the Commission if the Company omits the entire proposal from its proxy materials in reliance upon rule 14a-8(c)(7).

Finally, in *Union Pacific Corp.* (February 21, 2007), the Staff permitted exclusion of a proposal requesting information on the company's efforts to minimize financial risk arising from a terrorist attack or other homeland security incidents. The proposal was excludable in its entirety pursuant to Rule 14a-8(i)(7) as it related to the evaluation of risk, despite the proponent's objection that terrorism and homeland security raised significant social policy concerns. *See also Wal-Mart Stores, Inc.* (March 15, 1999) (permitting exclusion of a proposal requesting a report to ensure that the company did not purchase goods from suppliers using, among other things, forced labor, convict labor and child labor because the proposal requested that the report address ordinary business matters).

**C. The Proponents Improperly Rely on Precedents Which Relate to Proposals Focused on Censorship and Human Rights, Which Are Not the Subject Matters of the Proposal.**

As discussed above, in an after-the-fact effort to avoid exclusion of the Proposal on ordinary business grounds, the Proponents' Response Letter attempts to recast the focus of the Proposal in broad social and public policy terms. In particular, the Proponents' Response Letter refers to censorship and surveillance numerous times:

- “the core issues of  *censorship*  and  *privacy*  raised in the Proposal” (page 5) (emphasis added);
- “[t]urning to the subject matter of the proposal, ...  *censorship and surveillance*  by ISPs is a significant policy issue” (page 7) (emphasis added);
- “there is widespread public interest in  *censorship* ” (page 7) (emphasis added);
- “[o]n the issue of  *censorship*  concerns specifically, consider the  *censorship*  incident involving Verizon” (page 7) (emphasis added);
- “[c]onsider the enormous amount of mainstream media and business press coverage of the issue of  *surveillance* , network management and  *censorship* ” (page 7) (emphasis added);
- “[a]s demonstrated at length above, the issues of public expectations of  *privacy*  and  *censorship*  are significant social policies issues” (page 11) (emphasis added);
- “ *censorship*  and  *privacy*  expectations are becoming of greater interest to the public” (page 11) (emphasis added);
- “the Proposal seeks to address the significant  *privacy*  and  *censorship*  issues” (page 12) (emphasis added);
- “ *privacy*  and  *censorship*  issues are not excludable when they involve significant policy issues and focus on the company’s impacts” (page 12) (emphasis added); and
- “areas of our concern (the Company’s impact on public expectations of  *privacy*  and  *censorship* )” (page 18) (emphasis added).

While the Proponents’ Response Letter repeatedly refers to  *censorship*  as a main objective of the Proposal, nothing in the Proposal discusses or mentions “ *censorship* .” The Proponents are attempting to graft “ *censorship* ” and “ *surveillance* ” themes onto the Proposal in an effort to rely on  *Yahoo! Inc. (April 13, 2007)*  and  *Cisco Systems Inc. (July 13, 2002)* . Both were proposals focused on  *censorship*  and  *surveillance*  and were not excludable under Rule 14a-8(i)(7).

The  *Yahoo!*  proposal and supporting statement repeatedly referred to  *censorship*  by foreign governments, including protection of the identity of its customers in countries “where political speech can be treated as a crime” and the prevention of  *censorship*  by “authoritarian foreign governments.” Similarly, the proposal in  *Cisco*  related to

mentorship by governments, particularly China, and sought a report on company products that are sold to China or other governments, which allow monitoring and/or recording of Internet traffic and block Internet traffic from reaching recipients. Unlike the proposals in *Yahoo!* and *Cisco*, the Proposal does not request a report on mentorship, or on corporate activities that bear on mentorship. Rather, the focus of the Proposal is to report on Verizon's Internet network management practices and privacy policies. As a result, the Proponents' reliance on *Yahoo!* and *Cisco* is misplaced as these letters addressed matters which are not a focus of the Proposal.

The Proponents also attempt to rebut the numerous precedents cited in Section II.B.1. of the December 22 Letter by presenting immaterial or irrelevant distinctions and then concluding that the precedents are therefore inapplicable. For example, the Proponents disagree with Verizon's reliance on *AT&T Inc.* (February 7, 2008) and *Verizon Communications Inc.* (February 22, 2007). In each of these proposals, the proponent requested a report on the technical, legal and ethical policy issues pertaining to the disclosure of customer records and communications content to government agencies without a warrant and the effect of such disclosures on customer privacy rights. The Staff permitted exclusion of these proposals pursuant to Rule 14a-8(i)(7) because they implicated the company's ordinary business operations – procedures for protecting customer information. The Proponents' Response Letter argues, on page 13, that *AT&T* and *Verizon* are distinguishable because those proposals were "focused on customers and government surveillance while the Proposal is focused on the public and non-governmental surveillance" (emphasis in original). However, the Proponents fail to refute the argument that the report contemplated by the Proposal would still require Verizon to address its network management practices and customer privacy issues. As the Proponents' Response Letter acknowledges on page 13, "the focus of the Proposal is not on customer privacy or privacy policies, but rather on Internet network management practices and their impact on public expectations of privacy." As the Proposal would require an examination of Verizon's network management practices, it would intrude on Verizon's ordinary business operations and is therefore excludable under Rule 14a-8(i)(7).

Similarly, the Proponents' Response Letter, on page 13, attempts to refute the numerous precedents cited by Verizon in Section II.B.1. of the December 22 Letter, by claiming that such precedents "do not apply because they all expressly involved making explicit changes to specific compliance mechanisms or policy." The Proponents apparently argue that because the Proposal does not expressly ask Verizon to make explicit changes to its policies, the cited precedents fail to support Verizon's argument for exclusion under Rule 14a-8(i)(7). The Proponents appear to suggest that exclusion in the cited precedents was based on the fact that the proposal asked the company to make "explicit changes" to a policy. However, the basis for exclusion in each of those precedents was not that the proposal requested "explicit changes," but that the subject matter of the proposal dealt with the company's ordinary business operations. See,

*e.g.*, *H&R Block, Inc.* (August 1, 2006) (proposal related to ordinary business – “credit policies, loan underwriting, and customer relations”); *Bank of America Corp.* (March 3, 2005) (proposal related to ordinary business – “procedures for protecting customer information”); *Deere & Co.* (November 30, 2000) (proposal related to ordinary business – “customer relations”); *Associated First Capital Corp.* (February 23, 1999) (proposal related to ordinary business – “general conduct of a legal compliance program”); *Citicorp* (January 9, 1998) (proposal related to ordinary business – “initiation of a compliance program”).

**D. The Proponents Fail to Refute the Argument that the Proposal Involves Verizon’s Ordinary Business Operations.**

In objecting to Verizon’s ordinary business argument, the Proponents’ Response Letter incorrectly states, on page 11, that “the Company is arguing that privacy issues and freedom of speech issues are mundane matters that are fundamental to management’s ability to run a company on a day-to-day basis.” Verizon makes no such argument regarding privacy and freedom of speech. Rather, as discussed in Section II.B. of the December 22 Letter, Verizon regards the *development and implementation of policies and procedures* concerning customer privacy concerns and access to communications content as basic management functions and an integral part of Verizon’s day-to-day business operations.

Verizon’s operations include extensive and ongoing development and implementation of policies and procedures to manage Internet services that it provides to customers, including to protect the privacy of Verizon’s customers. The term “Internet network management practices” used in the Proposal is an enormously broad term that includes, among other things, terms of access, management of Internet traffic, broadband capacity, customer usage, management of online advertising, domain name systems and other matters routine to Verizon’s Internet business. The Proposal requests a report that would require Verizon to address the manner in which 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. Accordingly, the Proposal, on its face, relates to the day-to-day management functions of developing and implementing policies and procedures surrounding the protection of customer information. This defect cannot be cured by the Proponents’ repeated efforts to recast the requested report as an “examination of freedom of speech and privacy issues.” A report that focuses on Verizon and its protection of customer information is not a significant policy issue. It is a report relating to Verizon’s ordinary business operations. As noted in Section II.B.1. of the December 22 Letter, the Staff has long recognized that matters of customer privacy in general are necessarily part of a company’s ordinary business operations.

**E. The Proponents' Response Letter Supports Verizon's Argument that the Proposal Is Inherently Vague and Indefinite.**

As noted above, the Proponents reframe and recast the Proposal and the purpose of the Proposal in the following ways throughout the Proponents' Response Letter:

- "an *examination* of freedom of speech and privacy issues" (page 3) (emphasis in original);
- "an *examination* of free speech and privacy issues ... that implicitly calls for a presentation of differing ideas and approaches" (page 4) (emphasis in original);
- "an exploration of the issues in the context of significant policy concerns and how they apply to the Company's future" (page 4);
- "a discussion or exploration of the impact the company has on our national values of privacy and free speech" (page 4);
- "the focus of the Proposal is not on customer privacy or privacy policies, but rather on Internet network management practices and their impact on public expectations of privacy" (page 13);
- "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" (page 13);
- "the Proposal is focused on an examination of 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" (page 13);
- "an examination of the Company's impact on social goods such as public expectations of privacy and freedom of speech" (page 13);
- "the negative impacts, real and potential, of Verizon's Internet management activities on fundamental societal values such as privacy and free speech" (page 14);
- "the Proposal seeks a discussion of how the Company will impact society" (page 15);

- “the Proposal expressly seeks an examination of public policy issues and impacts on society” (page 17);
- “[the Proposal] 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” (page 17) (emphasis in original);
- “[i]t is about how the Company impacts our human rights” (page 17); and
- “[w]e are intending this report to be an examination of *how the Company has an impact on our society* and how privacy interests are impacted by commercial interests” (page 18) (emphasis added).

To the extent that the Proponents are seeking to engage Verizon in a philosophical debate of privacy rights and freedom of speech, the requested report is so inherently vague and indefinite that it violates Rule 14a-8(i)(3) and Rule 14a-8(i)(6). It is evident that the Proponents recognize this substantial defect by asserting, on page 17 of the Proponents’ Response Letter, without support or justification, that the Proposal has “struck a reasoned and appropriate balance” between crafting a proposal that is neither “too detailed” nor “too vague.” However, the Proponents’ bare statement that the Proposal has struck the proper balance does not make it so and cannot overcome the inherent defects of the Proposal. The Proposal, as evidenced by the various formulations and interpretations in the Proponents’ Response Letter, is subject to multiple interpretations such that it would be impossible for shareholders voting on the Proposal to determine with any reasonable certainty exactly what actions or measures the Proposal intends or requires. Similarly, it would be impossible for Verizon, in implementing the Proposal (if adopted), to determine with any reasonable certainty exactly what information should be contained in the required report. As a result, the Proposal is inherently vague and indefinite and excludable pursuant to Rule 14a-8(i)(3).

Although the Proponents object to a company arguing exclusion pursuant to both Rule 14a-8(i)(3) and Rule 14a-8(i)(10), the two arguments are not mutually exclusive. The fact that Verizon believes it has substantially implemented the Proposal, in a manner satisfactorily addressing the essential concerns of the Proposal, is not inconsistent with the position that the Proposal itself is inherently vague or indefinite.

**F. Trillium Failed to Timely Supply Documentary Support Evidencing Satisfaction of the Eligibility Requirements of Rule 14a-8(b) and Therefore the Trillium Proposal Is Excludable Pursuant to Rule 14a-8(f).**

The Proponents’ Response Letter states that Trillium sent to Verizon a letter dated October 10, 2008 signed by Mr. Ames authorizing Trillium to act on his behalf and specifying the number of shares Mr. Ames owns (the “Ames Authorization Letter”).

The Proponents' Response Letter, on page 19, states that the Ames Authorization Letter was sent to Verizon via facsimile transmission on November 26, 2008 and via courier on December 1, 2008. While Verizon received other correspondence from Trillium at that time, it did not receive a copy of the Ames Authorization Letter until January 20, 2009, when it received a copy of the Proponents' Response Letter.<sup>2</sup>

As discussed in Section II.D. of the December 22 Letter, the Trillium Proposal is deficient because the letter from Charles Schwab & Company did not specify the number of shares in Mr. Ames' account and only stated that Mr. Ames' stock is worth more than \$2,000. As a result, Verizon was unable to confirm whether the \$2,000 minimum ownership requirement under Rule 14a-8(b) had been satisfied since it could not verify the market value of the securities as prescribed under Section C.1.a. of SLB No. 14. Because Verizon did not receive a copy of the Ames Authorization Letter until long after the 14-day response period had expired, the Trillium Proposal is excludable because Trillium failed to timely supply documentary support evidencing its satisfaction of Rule 14a-8(b).

The Proponents' Response Letter erroneously concludes that "[t]here is no requirement ... that the number of shares be enumerated" by relying on Staff guidance addressing a different aspect of Rule 14a-8(b), that is, the "continuous ownership" requirement. Specifically, the Proponents rely on Section C.1.c. of SLB No. 14 and Rule 14a-8(b)(2)(i), which only address the requirement to verify that the shareholder has owned the securities "continuously for one year." Trillium improperly concludes that because the provisions regarding "continuous ownership" do not discuss disclosure of the number of shares owned, that such disclosure is not required. Trillium reiterates its flawed analysis by further reasoning that because a broker statement "is essentially information about the number of shares" and the Staff "has indicated that documenting the number of shares through a statement is inadequate" with respect to proving continuous ownership, a shareholder is not required to specify his or her number of shares to the company. The fact that a broker's monthly or quarterly statements are inadequate to prove "continuous ownership," does not lead to the conclusion that disclosure of the number of shares is unnecessary. On the contrary, in order to comply with the calculation of market value of securities pursuant to Section C.1.a. of SLB No. 14, Verizon would need to know the number of shares owned by a proponent to calculate market value. Because Verizon did not receive this information until January 20, 2009, Trillium's response was not timely and therefore Trillium's Proposal is excludable pursuant to Rule 14a-8(f).

---

<sup>2</sup> The Ames Authorization Letter received by Verizon on January 20, 2009 is dated October 14, 2008, not October 10, 2008.

**G. The Proponents Fail to Establish that the Proposal Is Co-Sponsored and Therefore the Trillium Proposal May Be Excluded Because It Substantially Duplicates the Haible Proposal.**

The Proponents' Response Letter asserts, on page 20, that "Trillium Asset Management is clearly a co-filer" with Mr. Haible, but provides no evidence to support this assertion. There is nothing in the Trillium Proposal or the Haible Proposal or the related correspondence, prior to the Proponents' Response Letter, which states that Trillium and Mr. Haible are co-sponsors of the Proposal. Indeed, the Haible Proposal, which Verizon received on November 12, 2008, fails to state that Trillium or Mr. Ames are co-sponsors of the Proposal. Likewise, the Trillium Proposal, which Verizon received on November 17, 2008, fails to state that Mr. Haible is co-sponsor of the Proposal. The Proponents appear to regard co-sponsorship as self-evident by referring to the "obvious intent of the Proponents to co-file the Proposal." However, the absence of any documentary support stating that the parties are co-filers belies the Proponents' "obvious intent" argument.

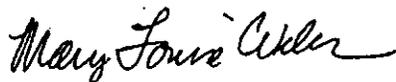
Accordingly, the Proponents have failed to provide evidence that Mr. Haible and Trillium are co-sponsors of the Proposal and the Trillium Proposal may be excluded pursuant to Rule 14a-8(i)(11) if the Haible Proposal is included in the 2009 proxy materials.

**III. Conclusion.**

For the reasons set forth above and in the December 22 Letter, Verizon continues to believe that the Proposal may properly be omitted from the 2009 proxy materials pursuant to Rule 14a-8(i)(7), Rule 14a-8(i)(10), Rule 14a-8(i)(3) and Rule 14a-8(i)(6) and requests the Staff's concurrence with its views. In addition, Verizon continues to believe that the Trillium Proposal may properly be omitted from the 2009 proxy materials pursuant to Rule 14-8(f) and, if the Haible Proposal is included in the 2009 proxy materials, under Rule 14-8(i)(11).

If you have any questions with respect to this matter, please telephone me at (908) 559-5636.

Very truly yours,



Mary Louise Weber  
Assistant General Counsel

cc: Mr. Paul Haible  
Mr. Jonas Kron, Trillium Asset Management Corporation  
Mr. Richard Ames

January 20, 2008

VIA e-mail: [shareholderproposals@sec.gov](mailto: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 Verizon Communications Inc. for 2009 Proxy Statement

Dear Sir/Madam:

This letter is submitted on behalf of Paul Heible, Richard Ames, and Trillium Asset Management Corporation (hereinafter referred to as "Proponents"), who are beneficial owners of shares of common stock of Verizon Communications Inc. (hereinafter referred to as "Verizon" or the "Company"), and who have jointly submitted a shareholder proposal (hereinafter referred to as "the Proposal") to Verizon, to respond to the letter dated December 22, 2007 sent to the Office of Chief Counsel by the Company, in which Verizon contends that the Proposal may be excluded from the Company's 2009 proxy statement by virtue of Rules 14a-8(i)(10), 14a-8(i)(7), 14a-8(i)(3), 14a-8(i)(6), 14a-8(f), and 14a-8(b).

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 Verizon'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, (2) the requested report is not moot, and (3) the Mr. Ames has meet the ownership requirements of the Rule. 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 the Company's Assistant General Counsel, Ms. Mary Louise Weber, at [mary.l.weber@verizon.com](mailto:mary.l.weber@verizon.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. This issue was the subject of a November 30<sup>th</sup> story in the New York Times in which the author, Professor Jeffery Rosen of George Washington University Law School said

#### **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

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...

Shareholders are rightly concerned about the strategic implications of these developments on the company and society. Verizon's management, however, 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 Verizon 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 21<sup>st</sup> 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 come under public scrutiny by consumer and civil liberties groups, regulatory authorities and shareholders;

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.

#### **The Company has not substantially implemented the Proposal**

The Company claims that the Proposal's request has been substantially implemented through its privacy policies. However, based on a review of the policies 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:

- do not constitute an *examination* of freedom of speech and privacy issues;
- are not the result of a Board examination of these issues;

- are not presented in a single document; and
- are not prepared for a shareholder audience.

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

The Proponents have requested an *examination* of free speech and privacy 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 significant policy concerns and how they apply to the Company's future as a profitable and socially responsible company. Clearly Verizon's privacy policies do not do that. Rather, Verizon's privacy policies are declarative statements about how the company will address some of these issues, which constitute a limited amount of disclosure, but do not rise to the level of a discussion or exploration of the impact the company has on our national values of privacy and free speech.

Furthermore, the privacy policy is inadequate because it is intended to communicate information to *customers*, while the Proposal requests information for *shareholders*. This is not a minor distinction. The concerns of shareholders can be much broader (or narrower as the case may be) than the concerns of its customers.

The privacy policies presented by the Company also do not present the information in the same form as we request. The Proposal asks for a single report, while the Company points to three websites and we are aware of at least one additional website: <http://www.verizonwireless.com/b2c/globalText?contentType=globalContent>. We are asking the Company to provide shareholders with this discussion in a unified manner, rather than over multiple websites perhaps containing duplicative or contextually different 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 provided what we seek, 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 the company through 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 Verizon is correct to cite many cases for the conclusion that companies are required to "substantially implement" proposals rather than "fully implement" proposals, what is critical is that it must, at the very least, address the core concerns raised by the proposal. See *Dow Chemical Company* (February 23, 2005); *ExxonMobil* (March 24, 2003); *Johnson & Johnson* (February 25, 2003); *ExxonMobil* (March 27, 2002); and *Raytheon* (February 26, 2001). In all of these cases the Staff rejected company arguments and concluded that the company's disclosures were insufficient to meet the substantially implemented standard. The case of *Wendy's International* (February 21, 2006) provides a particularly comparable example of the Staff rejecting a company's argument that information provided on a website was sufficient. In *Wendy's* the company argued that it had provided the requested sustainability report on its website and that the information contained on the website was sufficient. The proponent successfully demonstrated that the website contained no documentation that 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 fully address the core issues of censorship and privacy 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.

#### **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 evidenced by statements made by the Company itself. On September 25, 2008, Verizon Executive Vice President Thomas J. Tauke testified before the U.S. Senate Committee on Commerce, Science and Transportation in response to inquiries about the use of deep packet inspection (an Internet filtering technology that enables data mining, eavesdropping, and censorship). (Exhibit A) At that hearing Mr. Tauke stated that these issues, raised "important issues surrounding online privacy ." He also acknowledged the justifiable interest of legislators, stating, "Consumers and policy makers want to understand what personal information is being collected and used for advertising purposes."

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.

On the issue of censorship concerns specifically, consider the censorship incident involving Verizon in September 2007, when Verizon Wireless denied a request by Nara 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.

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 B):

**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

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  
*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  
*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 case is irrelevant because Verizon does not engage in such activities. But that misses the core inquiry of 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 and the

subject of policy maker interest.

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](http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html)

Perhaps that is why companies like AT&T, Microsoft, MetLife, Intel, Facebook, GE, IBM, and Wal-Mart have taken a central role in establishing a new Washington, D.C.-based policy organization called the Future of Privacy Forum ([www.futureofprivacy.org](http://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 it cannot be an overstatement to say that a significant social policy issue is at stake here. Public expectations of privacy are clearly a significant policy issue – and the business community 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 make 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 United States Senate Committee on Commerce, Science and Transportation held the hearing previously discussed, entitled "Hearing on Broadband Providers and Consumer Privacy."

Finally, in December, a number of 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 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 provide substantial reinforcement of the point made by Congressional committees, 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 does not fall under the exclusions related to business conduct**

The Company argues that Proposal is improper because it seeks to govern business conduct that management is in the best position to address. In short, the Company is arguing that privacy issues and freedom of speech issues are mundane matters that are fundamental to management's ability to run a company on a day-to-day basis.

First, even if one were to concede that it is true, the SEC made it clear in the 1998 Interpretive Release that "proposals relating to such [mundane] matters but focusing on sufficiently significant social policy issues generally would not be considered to be excludable." As demonstrated at length above, the issues of public expectations of privacy and censorship are significant social policies issues that, in the words of the Commission, "transcend the day-to-day business matters and raise policy issues so significant that it would be appropriate for a shareholder vote." *Id.*

As 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. Verizon 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.

There is support for this conclusion in previous Staff no-action letters. In *Cisco Systems Inc.* (July 13, 2002), the proposal focused on 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 Verizon, 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*<sup>1</sup> and therefore must be included in the Company's proxy materials.

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 central arguments 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 no-action request must be denied.

Second, the *Yahoo!* proponents argued that their proposal was not excludable because serious public policy concerns had been raised in Congress and the executive branch. 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

---

<sup>1</sup> 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.

on these societal values. But turning to the no-action letters cited by the Company it is clear that those are also insufficient to block the Proposal.

In *AT&T Inc.* (February 7, 2008), the proposal focused on "the policy issues that pertain to disclosing customer records and the content of customer communications to federal and state agencies without a warrant, as well as the effect of such disclosures on privacy rights of customers." The most obvious difference between the Proposal and the *AT&T* proposal was that the *AT&T* proposal was focused on *customers* and *government surveillance* while the Proposal is focused on *the public* and *non-governmental surveillance*. Furthermore, the focus of the Proposal is not on customer privacy or privacy policies, but rather on 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. Our 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 and freedom of expression.

Furthermore, the Proposal is distinguishable from *AT&T* because the focus is not limited to the narrow subject of customer privacy or privacy policies. The Company's Internet network management practices affect many more people than simply customers because of the practice of "peering" in which Verizon'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. The same analysis holds for *Verizon Communications Inc.* (February 22, 2007).

With respect to the other cases cited by the Company it is clear that they do not apply because they all expressly involved making explicit changes to specific compliance mechanisms or policy at the respective companies: *H&R Block Inc.* (August 1, 2006); *Bank of America Corporation* (March 3, 2005); *Deere & Company* (November 30, 2000); *Associated First Capital Corporation* (February 23, 1999);<sup>2</sup> *Chrysler Corp.* (February 18, 1998); and *Citicorp* (January 9, 1998). In contrast, the Proposal is focused on an examination of 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 and does not direct the Company to adopt any specific compliance mechanism or policy.

As for *Bank of America Corp.* (February 21, 2006) and (March 7, 2005), those are different than the Proposal because they simply requested a mere cataloging of existing policies and procedures for ensuring confidentiality. This Proposal, in contrast, goes beyond such a day-to-day issue, and requests an examination of the Company's impact on social goods such as public expectations of privacy and freedom of speech. Our Proposal does not simply focus on a mundane matter like describing or disclosing existing policies or mere procedural issues, but rather focuses on the significant policy issues of the societal concerns facing the Company.<sup>3</sup> The same analysis applies as well to *Citicorp* (January 8, 1997) and *Consolidated*

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

<sup>3</sup> We also observe that in both *Bank of America* cases the proponent did not offer any discussion or analysis of Rule 14a-8(i)(7), but made a

*Edison Inc.* (March 10, 2003).

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

In summary, it is critical to place this Proposal in its proper context. The Internet network management practices of Verizon 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 minutiae of customer privacy policies, not the negative impacts, real and potential, of Verizon'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 Proposal does not seek to direct the Company's lobbying efforts**

The Company contends that the Proposal is intended to involve the Company in legislative debates about consumer privacy and Internet network management practices. Leaving aside the fact that Verizon is already involved in those debates as evidenced by its appearance before a Senate committee, and that significant policy issues are by definition issues that will be of interest to policy makers, it is clear that the Proposal is proper because it does not ask the Company to directly lobby on a specific issue. 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://www.sec.gov/news/speech/2008/spch081081jww.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.

Furthermore, it is also evident that 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 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

few conclusory statements in response to the no-action request. Consequently, that proposal did not generate a full consideration of the issues.

voluntarily proposed and adopted in the United States to prevent youth from smoking and buying our cigarettes in developing countries." was permissible); *Unocal* (April 3, 1998) (permitted proposal requesting a discussion of the costs associated with increasing lobbying by Unocal of federal and local legislatures and governments); and *American Electric Power* (January 21, 1987) (seeking "information describing and explaining AEP's involvement in supporting or opposing state or national legislative and regulatory efforts to reduce power plant emissions, including AEP's support of groups like Citizens for Sensible Acid Rain Control, the Utility Air Regulatory Group and other lobbying and advocacy organizations.")

This is in addition to the previously discussed case of *Yahoo! Inc.*, (April 13, 2007) in which the proponent demonstrated that the proposal focused on a significant social policy issue by citing a specific piece of legislation that addressed similar issues. Clearly, Congressional interest in an issue is evidence that a proposal is in fact appropriate for shareholder consideration.

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

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

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

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

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

Finally, *Pacific Enterprises* (February 12, 1996) was properly excluded because it directed the regulatory, legislative and legal departments to undertake highly specific steps related to deregulation – i.e., it asked the Company to directly lobby on a specific issue:

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

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

For the above reasons, we respectfully request the Staff conclude that the Proposal must be included in the Company's proxy materials.

**The Company's discussion of "touch[ing] upon a matter with public policy implications" is not an accurate description of Rule 14a-8**

Almost as an aside, the Company argues that even if the Proposal "may touch upon a matter with public policy implications" 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.

As was discussed at length earlier, it is clear that Verizon is currently facing a significant social policy issue. To imply that the Proposal merely touches upon a significant policy issue is misplaced and cannot provide sufficient reasons to overcome the Company's significant burden of persuasion to exclude the Proposal.

**Significant policy issue conclusion**

In the preceding sections we have fully refuted the Company's ordinary business arguments. But more importantly it is clear that the impact of our 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 core 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 discussed earlier, these issues are significant policy issues confronting the Company. As shareholders we are concerned that the Company is not sufficiently addressing these issues at a strategic level. The Company has become a gatekeeper 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 Proposal is not vague, but rather focuses at the appropriate level of specificity**

Under Rules 14a-8(i)(3) and 14a-9, proposals are not permitted to be "so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B (September 15, 2004) ("SLB 14B") However, the SEC has also made it clear that it will apply a "case-by-case analytical approach" to each proposal. Exchange Act Release No. 34-40018 (May 21, 1998) ("1998 Interpretive Release"). Consequently, the vagueness determination becomes a very fact-intensive determination in which the Staff has expressed concern about becoming overly involved. SLB 14B. Finally, the Staff stated in SLB 14B that "rule 14a-8(g) makes clear that *the company bears the burden of demonstrating that a proposal or statement may be excluded.*" *Id* (emphasis added).

As a general matter, it is clear that the micro-management exclusion and the vagueness exclusion present two poles on the spectrum of permissible proposals. To pass muster, a proposal can be neither too detailed nor can it be too vague. All shareholders who submit proposals must place their proposals within that spectrum and we have been very cognizant of those requirements. In view of the entirety of the facts and circumstances, we believe that we have struck a reasoned and appropriate balance, as the Rule demands.

This is best illustrated by a number of other cases presented to the Staff. In *Microsoft Corporation* (September 14, 2000) the Staff required inclusion of a proposal that requested the board of directors to implement and/or increase activity on eleven principles relating to human and labor rights in China. In that case, the company argued "phrases like 'freedom of association' and 'freedom of expression' have been hotly debated in the United States" and therefore the proposal was too vague. Similarly, Verizon's claims that our Proposal is meaningless because it seeks to address issues like "public expectations of privacy and freedom of speech on the Internet" and therefore should not succeed.

This is also true of a case such as *Yahoo!* (April 13, 2007), which survived a challenge on

vagueness. In that case, the proposal sought "policies to help protect freedom of access to the Internet". See also *Cisco Systems, Inc.* (Sep. 19, 2002) (Staff did not accept claim that terms "which allows monitoring," "which acts as a firewall," and "monitoring" were vague); and *Cisco Systems, Inc.* (Aug. 31, 2005) (Staff did not accept claim that term "Human Rights Policy" was vague).

We have also taken the step, within the significant length restrictions of the Proposal, of providing shareholders and the Board with some guidance as to what kind of examination we are seeking. In the Supporting Statement, we stated "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." While this sentence makes it clear that we are simply making a suggestion, it does allow the shareholders and the Board to get some additional insight into our expectations. We are intending this report to be an examination of how the Company has an impact on our society and how privacy interests are impacted by commercial interests. Given that we are limited to 500 words, we believe this represents an effective way to facilitate the understanding of shareholders and the Board.

Finally, it is not at all clear how the Company can argue the Proposal is too vague to implement, but then argue that they have implemented it (see above). If the Proposal is too vague then how do they know they implemented it? If they implemented the Proposal, then they know what information it seeks and therefore it cannot be considered too vague. We would suggest that the mental gymnastics required to subscribe to the Company's contorted argument should be quickly discarded in favor of the simple and logical conclusion that we have struck the appropriate balance between micro-management and vagueness. The Company should not be permitted to argue both sides of this issue and should be compelled to make a coherent argument. We have provided management and shareholders sufficient guidance on the areas of our concern (the Company's impact on public expectations of privacy and censorship) without dictating to the Board how it should engage in the examination or otherwise interfere with its discretion. Therefore, we respectfully request the Staff reject the Company's argument.

#### **The Proposal does not contain any false or misleading statements**

The Company contends that two statements in the Proposal are false and mislead in violation of the rules. The first is the Supporting Statement which reads "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." The Company contends that the statement implies that the Company currently engages in such activities.

Staff Legal Bulletin No. 14B made it clear that a statement can be modified or excluded only if the company demonstrates that the

statements directly or indirectly impugn character, integrity, or personal reputation, or directly or indirectly make charges concerning improper, illegal, or immoral conduct or association, without factual foundation; [or]

the company demonstrates objectively that a factual statement is materially false or misleading;

The Company has done neither. In fact it is arguing that the statement is problematic

because it potentially could be interpreted to mean that the Company engages in such activities. In Staff Legal Bulletin No. 14B the Staff stated that such arguments are not grounds for exclusion or modification, pointing out that "The company is not responsible for the contents of the shareholder proponent's proposal or supporting statement." It went on to express great displeasure with such assertions by stating that they believe such an argument is "not beneficial to participants in the process and diverts resources away from analyzing core issues arising under rule 14a-8."

The Company's argument diverts attentions away from the questions at hand. It is clear to any reader that the Supporting Statement is simply a form of guidance to shareholders and the Board and serves as an illustrative example to assist in evaluating the Proposal.

The same is true of the Company's complaint about the statement "Class action lawsuits in several states are challenging the propriety of ISPs' network management practices," which it argues leaves a false and misleading "impression." This is not an objection that the statement is objectively false as required by the Rule. In fact the statement is objectively true. Once again, the Company is making subjective arguments of interpretation that the Staff has explicitly rejected and disfavored. As a result, it is diverting attention away from the genuine issues of concern under Rule 14a-8.

#### **The Proponents have provided documentation of ownership as required by the Rule**

The Company contends that the Proponents have failed to document Mr. Ames's ownership adequately and failed to provide a written statement from Mr. Ames authorizing Trillium Asset Management Corporation to act on his behalf.

With respect to Mr. Ames authorizing Trillium Asset Management Corporation to act on his behalf we have attached as Exhibit C Mr. Ames's client authorization letter dated October 10, 2008. That letter was included in our reply to Verizon's request for verification of ownership received by the Company by fax on November 26, 2008 and sent Optima on December 1, 2008. Optima Tracking #B50063222687303 - <http://shipping.shipoptima.com/action/openTracking?trackingNumber=B50063222687303>. This document makes it clear that Mr. Ames has authorized Trillium to act on his behalf.

As for the contention that the Proponents have failed to document Mr. Ames's ownership, the Company's argument is that our response letter did not establish Mr. Ames held the requisite amount of shares - i.e. it did not specify the number of shares he holds. Staff Legal Bulletin No. 14 does not require the proponent to specify the number of shares. Staff Legal Bulletin 14.3.1.C requires that the proponent "submit a written statement from the record holder of the securities verifying that the shareholder has owned the securities continuously for one year as of the time the shareholder submits the proposal." There is no requirement therein that the number of shares be enumerated.

In fact, Rule 14a-8(b)(2)(i) states that the the first way to document ownership

is to submit to the company a written statement from the "record" holder of your securities (usually a broker or bank) verifying that, at the time you submitted your proposal, you continuously held the securities for at least one year. You must also include your own written statement that you intend to continue to hold the securities through the date of the meeting of shareholders.

Once, again there is no requirement that the proponent document the number of shares.

We also note that Staff Legal Bulletin 14.3.1.C (2) states that a custodian or broker statement is not sufficient to provide evidence of ownership. Given that a statement is essentially information about the number of shares an individual holds and the Staff has indicated that documenting the number of shares through a statement is inadequate, it is reasonable to conclude that there is no requirement to specify the number of shares.

The custodian of the shares, Charles Schwab Institutional, has verified clearly and unequivocally that Mr. Ames holds the requisite value of shares. But beyond any of these arguments it is clear that the Mr. Ames disclosed in his authorization letter (Exhibit C) that he holds 274 shares. If the Company has any serious question about the size of Mr. Ames's holdings it has been in possession of such information since at least November 26, 2008 and would be able to calculate the value of his holdings to its satisfaction.

Accordingly we respectfully request the Staff reject the Company's arguments as to Mr. Ames's ownership.

**Trillium Asset Management is clearly a co-filer**

Before concluding its no-action request, the Company drops in what appears to be an afterthought that Trillium's Proposal is excludable as substantially duplicative of the Haible Proposal. Of course the Trillium Proposal is identical to the Haible Proposal for the simple reason that it constitutes a co-filed proposal. This fact is abundantly clear to Verizon as evidenced by the lack of any serious argument made by the Company and by the obvious intent of the Proponents to co-file the Proposal. We respectfully request the Staff focus on the core issues raised by the no-action request and disregard this empty assertion.

**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](mailto: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](mailto:jkron@trilliuminvest.com).

Sincerely,



Jonas Kron,  
Senior Social Research Analyst

**Enclosures**

**cc:**

**John Harrington, Harrington Investments**

**Paul Haible**

**Richard Ames**

**Prepared Testimony of Verizon Executive Vice President Thomas J. Tauke  
U.S. Senate Committee on Commerce, Science and Transportation  
"Broadband Providers and Consumer Privacy"  
Thursday, September 25, 2008**

**Chairman Inouye, Ranking Member Hutchison and Members of the Committee: thank you for the opportunity to discuss the important concerns and perspectives surrounding consumer privacy in the area of online advertising.**

**Today, more than 60 million American homes are connected to the Internet via broadband, and the wide range of content, services, and applications online – most offered for free – draws more people online every day.**

**While Verizon does not rely on online advertising as a significant source of revenue, we recognize that it has been a key business model that has helped make the Internet a growth engine for the U.S. economy.**

**Yet, using consumers' web-surfing data to foster targeted online advertising raises complex and important issues surrounding online privacy. Consumers and policy makers want to understand what personal information is being collected and used for advertising purposes. They want to know what privacy and consumer protections are in place, and what choices are available to participate – or not – in behavioral advertising models.**

**In a rapidly changing and innovative environment like the Internet, maintaining consumer trust is essential. It is critical that consumers understand what forms of targeted online advertising their service**

providers and favorite websites employ. If certain practices cause consumers to believe that their privacy will not be protected, or their preferences won't be respected, they will be less likely to trust their online services, and the tremendous power of the Internet to benefit consumers will be diminished. So, maintaining consumer trust in the online experience is critical to the future success of the Internet.

With that in mind, let me begin by describing the online advertising techniques Verizon uses today over its wireline networks.

Verizon's online advertising involves the practices commonly accepted throughout the Internet, such as the use of cookies or ad delivery servers to provide advertising that is limited to users of Verizon's own services or websites. We also provide ad-supported search results to help consumers find the websites they are looking for when they mistype an address. These practices, which are neither new nor unique, improve consumers' interaction with our websites and services, and increase the relevance of the advertising displayed to our customers or to visitors of our sites.

One technology that has received attention of late is "packet inspection." To be clear, Verizon has not used – and does not use – packet inspection technology to target advertising to customers, and we have not deployed the technology in our wireline network for such purposes.

Packet inspection can be a helpful engineering tool to manage network traffic and enable online services and applications consumers may wish to use. The perceived problem with "packet inspection" is not the technology. Many useful technologies can be used for nefarious purposes.

**The problem arises if packet inspection is used to inappropriately track customers' online activity without their knowledge and consent and invade their personal privacy.**

**In fact, any technology that is used to track and collect consumer online behavior for the purposes of targeted advertising – regardless of which company is doing the collecting – should only be used with the customer's knowledge and consent in accordance with the law, a company's specific privacy policies, and the privacy principles outlined below.**

**Protecting our customers' privacy has long been, and will continue to be, a priority at Verizon. We are committed to maintaining strong and meaningful privacy protections for consumers in this era of rapidly changing technological advances. We are strong proponents of transparency and believe that consumers are entitled to know what kinds of information we collect and use, and should have ready access to effective tools that allow them to control the use of that information.**

**At Verizon we have worked to craft – and communicate to our customers – responsible policies aimed at protecting online privacy.**

**We can commit – and believe that all companies should commit – to a set of best practices in the area of online behavioral advertising. The principles and best practices should apply to all online companies regardless of their technology or the platform used. The principles underlying the consumer protection practices we support are these:**

**First, meaningful consent.**

Verizon believes that before a company captures certain Internet-usage data for targeted or customized advertising purposes, it should obtain meaningful, affirmative consent from consumers. Meaningful consent requires: 1) transparency, 2) affirmative choice, and 3) consumer control.

Transparency involves conspicuous, clearly explained disclosure to consumers as to what types of data are collected and for what purpose that data is being used, how that data is retained and for how long, and who is permitted access to the data.

Consumers would then be able to use these clear explanations to make an affirmative choice that their information can be collected and used for online behavioral advertising. Importantly, a consumer's failure to consent should mean that there is no collection and use of that consumer's information for online behaviorally targeted advertising based on tracking of the consumer's Internet usage.

Finally, consumer control means that consumers have an ongoing opportunity to make a different choice about behavioral advertising. In other words, should consumers at some later time choose not to participate in the behavioral advertising, there are equally clear and easy-to-use instructions to make that change. That preference should remain in effect unless and until the consumer changes it.

**Second, security practices.**

Any company engaged in tracking and collecting consumer online behavioral information must have appropriate access, security, and

**technological controls to guard against unauthorized access to any personal information.**

**Third, safeguards for sensitive information.**

**Special attention must be given to the protection of information of a sensitive nature (e.g., accessing medical web sites). This information should not be collected and used for online behavioral advertising unless specific, affirmative consent, and customer controls are in place to limit such use. Specific policies may be necessary to deal with this type of information.**

**Consistent with our long-standing policies and practices, Verizon also believes that the content of communications, such as e-mail, instant messages, or VoIP calls, should not be used, analyzed, or disclosed for purposes of Internet-based targeted advertising.**

**Fourth, certification.**

**It is critical that all participants in online advertising – ad networks, publishers, search engines, Internet service providers, browser developers and other application providers – commit to these common sense principles and best practices through a broad-based, third party coalition. To achieve this, we plan to work with stakeholders in the Internet and advertising arenas, including other companies, industry groups and policy organizations.**

**The focus of this coalition and the principles should be the protection of consumers, not the technology or applications that happen to enable the data collection. Widespread and uniform adoption of principles will greatly enhance the public trust, address expressed privacy concerns**

**regarding web tracking practices, and serve as a foundation for further discussion with policy makers and consumer groups.**

**We believe that companies engaged in online behavioral advertising should agree to participate in a credible, third-party certification process to demonstrate to consumers that they are doing what they say with regard to the collection and use of information for online behavioral advertising. This process would confirm that companies are complying with and respecting consumers' expressed choices regarding such data collection.**

**We believe a framework such as this is a rational approach that protects consumer privacy, while allowing the market for Internet advertising and its related products and services to grow.**

**Should a company fail to comply with these principles, we believe the Federal Trade Commission has authority over abuses in the privacy area and can take appropriate measures against companies that intentionally violate applicable consumer protection laws.**

**We hope to use the next few months to work with all players in the Internet space to create and agree to live by industry best practices for online advertising.**

**Thank you.**

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

Fax: 617 482 6179

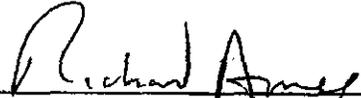
Dear Ms. Alpern:

I hereby authorize Trillium Asset Management Corporation to file a shareholder resolution on my behalf at Verizon (VZ).

I am the beneficial owner of 274 shares of Verizon (VZ) 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 no personal identifying information other than my name may appear on the corporation's proxy statement as the filer of the aforementioned resolution and will identify Trillium Asset Management Corporation's mailing address for the purposes of communicating information related to this shareholder resolution.

Sincerely,

  
Richard Ames  
c/o Trillium Asset Management Corporation  
711 Atlantic Avenue, Boston, MA 02111

10 / 14 / 08  
Date

Mary Louise Weber  
Assistant General Counsel



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

December 22, 2008

**By email to [shareholderproposals@sec.gov](mailto: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: Verizon Communications Inc. 2009 Annual Meeting  
Shareholder Proposals of Paul Haible and Trillium  
Asset Management Corporation

Ladies and Gentlemen:

This letter is submitted on behalf of Verizon Communications Inc., a Delaware corporation ("Verizon"), pursuant to Rule 14a-8(j) under the Securities Exchange Act of 1934, as amended. On November 12, 2008, Verizon received a shareholder proposal and supporting statement (the "Haible Proposal") from Paul Haible ("Mr. Haible") for inclusion in the proxy materials to be distributed by Verizon in connection with its 2009 annual meeting of shareholders (the "2009 proxy materials"). On November 17, 2008, Verizon received an identical shareholder proposal and supporting statement (the "Trillium Proposal") from Trillium Asset Management Corporation ("Trillium"), on behalf of certain of its clients, for inclusion in the 2009 proxy materials. Mr. Haible and Trillium are herein sometimes referred to collectively as the "Proponents," and the Haible Proposal and the Trillium Proposal are herein sometimes referred to collectively as the "Proponent." Copies of the Haible Proposal and all of the correspondence relating to it are attached as Exhibit A, and copies of the Trillium Proposal and all correspondence relating to it are attached as Exhibit B. For the reasons stated below, Verizon intends to omit the Haible Proposal and the Trillium Proposal from its 2009 proxy materials.

In accordance with Staff Legal Bulletin No. 14D (November 7, 2008), this letter is being submitted by email to [shareholderproposals@sec.gov](mailto:shareholderproposals@sec.gov). A copy of this letter is being sent by overnight courier to each of the proponents as notice of Verizon's intent to omit the Proposal from Verizon's 2009 proxy materials.

**I. Introduction.**

On November 12, 2008, Verizon received by facsimile transmission a letter dated November 12, 2008, from Mr. Haible submitting the following 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 21<sup>st</sup> 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, email 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;*
- *53% of Americans are uncomfortable with companies using their email content or browsing history to send relevant ads;*
- *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 come under public scrutiny by consumer and civil liberties groups, regulatory authorities and shareholders;*
- *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 issues 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.*

On November 17, 2008, Verizon received the identical proposal from Trillium.

Verizon believes that the Haible Proposal may be properly omitted from its 2009 proxy materials:

- under Rule 14a-8(i)(10) because Verizon has already substantially implemented the proposal;
- under Rule 14a-8(i)(7) because it deals with a matter relating to Verizon's ordinary business operations; and
- under Rules 14a-8(i)(3) and 14a-8(i)(6) because it is so inherently vague and indefinite that neither the shareholders voting on the proposal nor Verizon in implementing it (if adopted) would be able to determine with any reasonable certainty exactly what measures the proposal requires.

Verizon believes that the Trillium Proposal may be properly omitted from its 2009 proxy materials:

- under Rule 14a-8(i)(10) because Verizon has already substantially implemented the proposal;

- under Rule 14a-8(i)(7) because it deals with a matter relating to Verizon's ordinary business operations;
- under Rules 14a-8(i)(3) and 14a-8(i)(6) because it is so inherently vague and indefinite that neither the shareholders voting on the proposal nor Verizon in implementing it (if adopted) would be able to determine with any reasonable certainty exactly what measures the proposal requires; and
- under Rule 14a-8(f) because Trillium failed to provide documentary support that Trillium meets the eligibility requirements of Rule 14a-8(b).

Verizon respectfully requests the concurrence of the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission (the "Commission") that it will not recommend enforcement action against Verizon if Verizon omits the Haible Proposal and the Trillium Proposal, each in its entirety, from its 2009 proxy materials.

If the Staff is unable to agree that the Haible Proposal may be excluded from the 2009 proxy materials, then, in addition, Verizon believes it would be proper to exclude the Trillium Proposal from the 2009 proxy materials pursuant to Rule 14a-8(i)(11) because it substantially duplicates a previously received proposal (the Haible Proposal) that would be included in the 2009 proxy materials. In that event, Verizon respectfully requests the concurrence of the Staff that it will not recommend enforcement action against Verizon if Verizon omits the Trillium Proposal in its entirety from its 2009 proxy materials.

## **II. Bases for Excluding the Proposals.**

### **A. The Proposal May Be Excluded Under Rule 14a-8(i)(10), Because Verizon Has Substantially Implemented It.**

The Proposal calls for a report discussing Verizon's internet management practices in the context of the public's expectations of privacy and freedom of speech on the Internet. Verizon believes that it may exclude the Proposal under Rule 14a-8(i)(10) because Verizon has already substantially implemented the request of the Proposal by making extensive materials addressing these issues available on its corporate and Verizon Online websites set forth below.

The "substantially implemented" standard reflects the Staff's interpretation of the predecessor rule (allowing omission of a proposal that was "moot") that a proposal need not be "fully effected" by the company to meet the mootness test so long as it was "substantially implemented." See SEC Release No. 34-20091 (August 16, 1983). Pursuant to the 1983 interpretation, the Staff has stated that "a determination that the company has substantially implemented the proposal depends upon whether its particular policies, practices and procedures compare favorably with the guidelines of the proposal." *Texaco, Inc.* (March 28, 1991). See, also, *Nordstrom Inc.* (February 8, 1995 (proposal that company commit to code of conduct for overseas suppliers that

was substantially covered by existing company guidelines) and *The Gap, Inc.* (March 8, 1996) (same). Other Staff no-action letters have established that a company need not comply with every detail of a proposal in order to exclude it under Rule 14a-8(i)(10). Differences between a company's actions and a proposal are permitted so long as a company's actions satisfactorily address the proposal's underlying concerns.

Customer privacy issues are central to the success of each of Verizon's lines of business, and Verizon devotes substantial management resources to the development and implementation of policies and procedures that address customer privacy expectations. The home page of Verizon's internet website ([www.verizon.com](http://www.verizon.com)) contains a link entitled "Privacy Policy." That link brings the reader to Verizon's "Privacy and Customer Security Policies." Through additional links, readers may access numerous pages explaining Verizon's general privacy principles and specific policy and procedures with respect to internet privacy. The principles govern all aspects of how individual customer information is handled across Verizon's businesses, including how it is collected and used, how customers are informed of their rights, when and to whom customer information may be disclosed and how Verizon implements its privacy practices. Verizon's general privacy principles and policies and procedures for internet privacy can also be accessed from the homepage of Verizon Online's internet website ([www.verizononline.net](http://www.verizononline.net)). A copy of the general privacy principles and policies and procedures is attached as Exhibit C.

Verizon has adopted a set of core principles with respect to its treatment of communications content provided over its networks. These guidelines, which can be found at <http://responsibility.verizon.com/home/contentpolicy/>, offer Verizon's customers, business partners and others interested in its views on content management insight into how Verizon views and approaches the important policy issues involving content. The guidelines address freedom of expression, the use of ratings and other standards, and the use and availability of parental controls and other means Verizon makes available to help its customers control the content that they and their families can access and view over Verizon's network. A copy of these guidelines and Verizon's content management policies is attached as Exhibit D.

Verizon believes that all of these publicly available materials, taken together, substantially implement the Proposal's request for a report discussing Verizon's internet management practices in the context of user expectations and rights regarding privacy and freedom of speech. Because the materials clearly address the underlying concern expressed by the Proposal, Verizon is of the view that the Proposal may be properly omitted from its 2009 proxy materials pursuant to Rule 14a-8(i)(10).

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

Rule 14a-8(i)(7) permits a company to omit a shareholder proposal from its proxy materials if it deals with a matter relating to the company's ordinary business

operations. Exchange Act Release No. 34-12999 (November 22, 1976). The general policy underlying the "ordinary business" exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting." Exchange Act Release No. 34-40018 (May 21, 1998). This general policy reflects two central considerations: (i) "[c]ertain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight"; and (ii) the "degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." Exchange Act Release No. 34-40018 (May 21, 1998) (the "1998 Release"). Verizon believes that these policy considerations clearly justify exclusion of the Proposal. The development and implementation of policies and procedures surrounding customer privacy concerns and access to communications content are basic management functions and an integral part of Verizon's day-to-day business operations as a telecommunications company and Internet service provider. The protection of customer information and privacy rights and access to communications content are the subject of evolving laws and regulations, as well as a rapidly evolving technological landscape, and, as such, as stated in the 1998 Release, are precisely the type of matter "of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment."

*1. The Proposal Impermissibly Seeks to Subject Basic Management Functions – Protecting Customer Privacy and Network Management Practices – to Shareholder Oversight.*

The Staff has long recognized that proposals which attempt to govern business conduct involving internal operating policies, customer relations and legal compliance programs may be excluded from proxy materials pursuant to Rule 14a-8(i)(7) because they infringe upon management's core function of overseeing business practices. See, e.g., *AT&T Inc.* (February 7, 2008) and *Verizon Communications Inc.* (February 22, 2007), where in each case the proposal requested a report on the technical, legal and ethical policy issues pertaining to the disclosure of customer records and communications content to government agencies without a warrant and the effect of such disclosures on customer privacy rights. See also *H&R Block Inc.* (August 1, 2006) (proposal sought implementation of legal compliance program with respect to lending policies); *Bank of America Corporation* (March 3, 2005) (proposal to adopt a "Customer Bill of Rights" and create a position of "Customer Advocate"); *Deere & Company* (November 30, 2000) (proposal relating to creation of shareholder committee to review customer satisfaction); *CVS Corporation* (February 1, 2000) (proposal sought report on a wide range of corporate programs and policies); *Associates First Capital Corporation* (February 23, 1999) (proposal requested that Board monitor and report on legal compliance of lending practices); *Chrysler Corp.* (February 18, 1998) (proposal requesting that board of directors review and amend Chrysler's code of standards for its international operations and present a report to shareholders); *Citicorp* (January 9,

1998) (proposal sought to initiate a program to monitor and report on compliance with federal law in transactions with foreign entities).

The Staff's no-action letters have expressly found that policies and procedures for protection of customer information are basic customer relations matters. For example, in *Bank of America Corporation* (February 21, 2006), the Staff permitted exclusion pursuant to Rule 14a-8(i)(7) of a proposal seeking a report on policies and procedures for protecting customer information. See also *Bank of America Corporation* (March 7, 2005) (same); *Consolidated Edison Inc.* (March 10, 2003) (proposal sought to govern how employees should handle private information obtained in the course of employment); and *Citicorp* (January 8, 1997) (proposal requested report on policies and procedures to monitor illegal transfers through customer accounts).

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

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

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

proposal calling for an evaluation of the impact on the company of various federal healthcare proposals); *Dole Food Company* (February 10, 1992) (same); and *GTE Corporation* (February 10, 1992) (same).

In *International Business Machines, supra*, the Staff's letter allowing exclusion of the proposal specifically noted that "the proposal appears directed at involving IBM in the political or legislative process relating to an aspect of IBM's operations." Here, the Proponents clearly want to utilize the resources of Verizon and the platform of its proxy statement to involve Verizon in the ongoing legislative debate about consumer privacy rights and Internet network management practices. The Proposal falsely suggests that Verizon has been complicit in violations of customer privacy, including the tracking and profiling of users' online behavior for profit and the collection and sale of personal information to third parties. On a day-to-day basis Verizon devotes substantial resources to monitoring compliance with laws relating to its handling of customer information, cooperating with lawful requests for information from law enforcement agencies and others and actively participating in ongoing regulatory, legislative and judicial proceedings relating to privacy issues, access to communications content and network management practices. The Proposal inappropriately seeks to intervene in Verizon's routine management of this basic area of its business in order to advance a specific political or legislative objective.

The fact that a proposal may touch upon a matter with public policy implications does not necessarily remove it from the realm of ordinary business matters. Rather, no action precedents demonstrate that the applicability of Rule 14a-8(i)(7) depends largely on whether implementing the proposal would have broad public policy impacts outside the company or would only deal with matters of the company's internal business operations, planning and strategy. For example, in *Microsoft Corporation, supra*, the Staff permitted exclusion of a proposal relating to a significant policy issue (i.e., net neutrality), because it recognized that evaluating the impact of expanded government regulation of the internet was a matter of the company's internal business operations, planning and strategy. As discussed above, implementing the Proposal would clearly involve matters central to Verizon's internal business operations, planning and strategy.

For all of the foregoing reasons, Verizon believes that the Proposal may be omitted from its 2009 proxy materials because it deals with matters relating to Verizon's ordinary business operations.

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

1. *The Proposal is So Inherently Vague and Misleading that Verizon Would be Unable to Determine What Action Should be Taken.*

Notwithstanding the fact that Verizon believes that Verizon's publicly available materials substantially implement the request of the Proposal under Rule 14a-8(i)(10),

Verizon also believes that the Proposal may be properly excluded under Rule 14a-8(i)(3) and Rule 14a-8(i)(6), because the description of the requested report is so vague and indefinite that "any action ultimately taken by the Company upon implementation of the proposal could be significantly different from the actions envisioned by the shareholders voting on the proposal." *Fuqua Industries, Inc.* (March 12, 1991).

Rule 14a-8(i)(3) permits a company to omit a shareholder proposal and the related supporting statement from its proxy materials if such "proposal or supporting statement is contrary to any of the Commission's proxy rules, including Rule 14a-9, which prohibits materially false or misleading statements in proxy soliciting materials." According to the Staff, a proposal will violate Rule 14a-8(i)(3) when "the resolution contained in the proposal is so inherently vague or indefinite that neither the stockholders voting on the proposal, nor the company in implementing the proposal (if adopted), would be able to determine with any reasonable certainty exactly what actions or measures the proposal requires." Staff Legal Bulletin No. 14B Section B.4. (September 15, 2004). See, also, *FirstEnergy Corp.* (February 18, 2004) (permitting exclusion of proposal urging Board to change company's governing documents relating to shareholder approval of shareholder proposals, because requested vote requirement was vague and misleading); *Global Entertainment Holdings/Equities, Inc.* (July 10, 2003) (permitting omission of a proposal that Board adopt an "action plan" which "accounts" for past sale of a business and resulting licensing arrangements, because it was vague and indefinite); *Pfizer Inc.* (February 18, 2003) (permitting omission of a proposal requesting board make all stock options at no less than the "highest stock price" and that the stock options contain a buyback provision, because action requested was vague and indefinite); *Johnson & Johnson* (February 7, 2003) (permitting omission of a shareholder proposal that called for a report on the company's "progress with the Glass Ceiling Report", but did not explain the substance of the report); *H.J. Heinz Co.* (May 25, 2001) (permitting omission of a shareholder proposal under Rule 14a-8(i)(3) where the proposal requested the company to implement the SA8000 Social Accountability Standards, but did not clearly set forth what SA8000 required of the company); *Kohl's Corp.* (March 13, 2001) (same); and *Philadelphia Electric Co.* (July 30, 1992) (permitting omission of a shareholder proposal under predecessor Rule 14a-8(c)(3) where a proposal resolved that a committee of small stockholders would refer a "plan or plans" to the board, but did not describe the substance of those plans). In addition, a company may exclude a shareholder proposal under Rule 14a-8(i)(6) if it is beyond the company's power to implement it. A company lacks the power or authority to implement a proposal under Rule 14a-8(i)(6) when the proposal in question "is so vague and indefinite that [the company] would be unable to determine what action should be taken." *International Business Machines Corporation* (January 14, 1992).

Like the proposals described above, the Proposal may be properly excluded from Verizon's 2009 proxy materials because the scope and focus of the requested report is so vague and indefinite that it is open to myriad interpretations. By generically referring to the "public's expectations of privacy and freedom of speech on the Internet" without providing parameters defining those expectations, the Proposal

fails to provide any point of reference for the report. For example, an individual who joins a social networking site, shares music and videos online or participates in a blog is likely to have very different expectations as to privacy and freedom of speech on the Internet than another individual who solely uses the internet to engage in online shopping or banking transactions or a third individual who wants to view illicit adult material or a fourth individual who is concerned about her child being able to access that material. The possible scenarios for what constitutes the "public's expectations" are countless. As a result, it would be impossible for either the shareholders or the Verizon Board to ascertain precisely what implementation of the Proposal would entail. Verizon is being asked to dedicate valuable analytical resources to a hypothetical, ill-defined study, not to a corporate report to shareholders.

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

***2. The Entire Supporting Statement and Portions of the Preamble are False and Misleading in Violation of Rule 14a-9***

There is a materially false and misleading implication in the Proposal and supporting statement that Verizon engages in network management practices that it actually prohibits. For example, the supporting statement suggests that the requested report could examine the "social and political effects of collecting and selling personal information to third-parties, including information companies such as First Advantage and Equifax", but does not explain that Verizon has a publicly-disclosed policy *against* collecting and selling personal information. In addition, the statement in the preamble that "Class action lawsuits in several states are challenging the propriety of ISPs' network management practices" creates the false and misleading impression that the propriety of Verizon's network management practices has been challenged in class actions lawsuits, when this is not the case. If the Proposal is not omitted in its entirety, Verizon believes that the entire supporting statement and the portion of the preamble discussed above may be omitted because they are materially false and misleading in violation of Rule 14a-9.

**D. The Trillium Proposal May be Excluded from the 2009 Proxy Materials Pursuant to Rule 14a-8(f) Because Trillium Failed to Supply Documentary Support Evidencing Satisfaction of the Eligibility Requirements of Rule 14a-8(b)**

Rule 14a-8(b)(1) provides that, in order to be eligible to submit a proposal, a shareholder must have continuously held at least \$2,000 in market value, or 1%, of the company's securities entitled to be voted on the proposal for at least one year prior to the date the proposal is submitted and must continue to hold those securities through the date of the meeting. If the proponent is not a registered holder, he or she must provide proof of beneficial ownership of the securities and also include a written statement that he or she intends to continue to hold the securities through the date of the meeting of shareholders. Under Rule 14a-8(f)(1), a company may exclude a shareholder proposal if the proponent fails to provide evidence that it meets the eligibility requirements of Rule 14a-8(b), provided that the company timely notifies the proponent of the deficiency and the proponent fails to correct the deficiency within the required time.

Verizon received the Trillium Proposal by Federal Express on November 17, 2008. The submission did not include documentation establishing that the Proponent had met the eligibility requirements of Rule 14a-8(b)(1). Instead, Trillium stated in a letter dated November 14, 2008, which accompanied the Proposal, that "Trillium submits this proposal on behalf of our clients, who are the beneficial owners, per Rule 14a-8, of more than \$2,000 worth of Verizon Communications Inc. common stock acquired more than one year prior to this date." No such clients were identified by name or otherwise, and no information was provided as to the number of Verizon shares owned by such clients individually or in the aggregate. Referring to the unidentified clients, the letter also states "They have stated their intention to hold this position throughout the date of the next annual stockholder meeting in 2009." After determining that Trillium was not a shareholder of record, in accordance with Rule 14a-8(f)(1) on November 21, 2008, Verizon sent a letter to the Proponent via Federal Express (the "Notification Letter") requesting the names of the proponents whom Trillium was representing, together with a written statement from each proponent authorizing Trillium to act on such proponent's behalf with respect to the submission of the proposal. The Notification Letter also requested a written statement from the record owner of each proponent's shares verifying that the proponent beneficially owned the requisite number of shares of Verizon stock continuously for at least one year prior to the date of submission of the Trillium Proposal. The Notification Letter advised the Trillium that such documentation had to be submitted to Verizon within 14 days of the Trillium's receipt of such letter. As suggested in Section G.3 of Division of Corporation Finance: Staff Legal Bulletin No. 14 (July 13, 2001) ("SLB No. 14") relating to eligibility and procedural issues, the Notification Letter included a copy of Rule 14a-8. Verizon received confirmation from Federal Express that the Notification Letter was delivered to Trillium on November 24, 2008. A copy of the Notification Letter is attached as Exhibit E to this letter.

On November 26, 2008, Verizon received by facsimile transmission a letter dated November 26, 2008 (the "Response Letter") from Charles Schwab & Company ("Schwab"), referencing Richard Ames and a specified Schwab account number (redacted for purposes of this letter). The Schwab letter verified that Schwab holds as custodian for Mr. Ames's account more the \$2,000 worth of common stock in Verizon Communication s Inc. and that these shares have been held continuously for at least one year prior to and through November 17, 2008. A copy of the Response Letter is attached as Exhibit F to this letter. Verizon received no further correspondence from Trillium, Mr. Ames or Schwab.

Although the Response Letter was timely sent to Verizon, it did not satisfy the requirements of Rule 14a-8(b). Pursuant to such Rule, the proponent was required to submit a written statement from the record holder of his shares, verifying his continuous ownership of *at least \$2,000* of Verizon shares from November 17, 2007 through November 17, 2008. While the Response Letter verifies that Mr. Ames held Verizon stock for the requisite period, it fails to establish that he held the requisite amount of Verizon stock to satisfy the \$2,000 threshold. In Section C.1.a. of SLB No. 14, the Staff explains how to calculate the market value of securities for purposes of Rule 14a-8(b) :

**a. How do you calculate the market value of the shareholder's securities?**

Due to market fluctuations, the value of a shareholder's investment in the company may vary throughout the year before he or she submits the proposal. In order to determine whether the shareholder satisfies the \$2,000 threshold, we look at whether, on any date within the 60 calendar days before the date the shareholder submits the proposal, the shareholder's investment is valued at \$2,000 or greater, based on the average of the bid and ask prices. Depending on where the company is listed, bid and ask prices may not always be available. For example, bid and ask prices are not provided for companies listed on the New York Stock Exchange. Under these circumstances, companies and shareholders should determine the market value by multiplying the number of securities the shareholder held for the one-year period by the highest *selling* price during the 60 calendar days before the shareholder submitted the proposal. For purposes of this calculation, it is important to note that a security's highest selling price is not necessarily the same as its highest closing price.

The Response Letter merely confirms that, as of November 26, 2008, the stock in Mr. Ames account is worth more than \$2,000. However, because the Response Letter does not specify the number of shares in Mr. Ames account, Verizon cannot confirm that these shares satisfied the \$2,000 threshold on any date within the 60 calendar days before November 17, 2008.

Trillium also failed to provide a written statement from Mr. Ames authorizing Trillium to act on his behalf with respect to the Proposal. Absent such an authorization,

Verizon has no way to confirm that Trillium is indeed authorized to submit the proposal on his behalf or to represent that Mr. Ames will continue to hold the requisite amount of Verizon stock through the date of the annual meeting.

The Staff has consistently taken the position that if a proponent does not provide on a timely basis documentary support sufficiently evidencing that it has satisfied the requirements of Rule 14a-8(b), the proposal may be excluded under Rule 14a-8(f). See, e.g., *General Motors Corporation* (April 5, 2007) (account summary insufficient verification of continuous ownership); *Yahoo! Inc.* (March 29, 2007) (broker's letter did not specifically verify continuous ownership); *The Home Depot, Inc.* (February 5, 2007) (broker's letter verifying ownership "for the past year" was insufficient to provide proof of ownership for requisite period); *General Electric Company* (January 16, 2007) (brokerage statement insufficient); and *International Business Machines Corporation* (November 16, 2006) (broker's letter dated before date of submission did not verify continuous ownership for requisite period).

While Rule 14a-8(f) requires a company receiving a proposal to notify the proponent of any procedural or eligibility deficiencies, it does not require a second notification if the response to the first notification was deficient. Any further verification Trillium or Mr. Ames might now submit would be untimely under Rule 14a-8(f). Therefore, Verizon believes that the Trillium Proposal is excludable pursuant to Rule 14a-8(f) because Trillium failed to remedy the eligibility deficiency on a timely basis after notification by Verizon.

**E. The Trillium Proposal May be Excluded From Verizon's 2009 proxy Materials Pursuant to Rule 14a-8(i)(11) Because It Substantially Duplicates the Haible Proposal**

Under Rule 14a-8(i)(11), a proposal may be omitted "[i]f the proposal substantially duplicates another proposal previously submitted to the company by another proponent that will be included in the company's proxy materials for the same meeting." The Trillium Proposal is identical to the Haible Proposal, which was received by Verizon five days prior to the Trillium Proposal. Accordingly, if the Staff concludes that the Haible Proposal cannot be excluded from Verizon's 2009 proxy materials under any of the bases set forth in this request and Verizon includes it in its 2009 proxy materials, then Verizon believes that the Trillium Proposal may be excluded as substantially duplicative of the Haible Proposal.

**III. Conclusion.**

Verizon believes that both the Haible Proposal and the Trillium Proposal may be omitted from its 2009 proxy materials (1) under Rule 14a-8(i)(10) because Verizon has already substantially implemented the request of the Proposal; (2) under Rule 14a-8(i)(7) because the Proposal deals with matters relating to Verizon's ordinary business operations and (3) under Rules 14a-8(i)(3) and 14a-8(i)(6) because the Proposal is

U.S. Securities and Exchange Commission  
Division of Corporation Finance  
Office of the Chief Counsel  
December 22, 2008  
Page 14

inherently vague and indefinite. Accordingly, Verizon respectfully requests the concurrence of the Staff that it will not recommend enforcement action against Verizon if Verizon omits both the Haible Proposal and the Trillium Proposal, each in its entirety, from Verizon's 2009 proxy materials.

In addition, Verizon believes that the Trillium Proposal may be omitted from its 2009 proxy materials (1) under Rule 14a-8(f) because Trillium failed to provide documentary support evidencing compliance with Rule 14a-8(b) and, (2) if the Haible Proposal is included in the 2009 proxy materials, under Rule 14a-8(i)(11) because the Trillium Proposal substantially duplicates a prior received proposal. Accordingly, Verizon respectfully requests the concurrence of the Staff that it will not recommend enforcement action against Verizon if Verizon omits the Trillium Proposal in its entirety from its 2009 proxy materials.

If you have any questions with respect to this matter, please telephone me at (908) 559-5636.

Very truly yours,



Mary Louise Weber  
Assistant General Counsel

Enclosures

cc: Mr. Paul Haible  
Mr. Jonas Kron, Trillium Asset Management Corporation

Paul Haible

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

November 12, 2008

Mr. Ivan G. Seidenberg

Chairman and CEO

Verizon Communications Inc.  
140 West Street  
New York, NY 10007

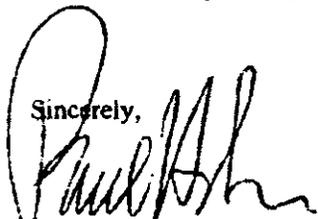
Re: Shareholder Resolution

Dear Mr. Seidenberg:

I have serious concerns regarding the practice of Internet filtering and the impact it can have on participation, expression, competition and innovation on the Internet. I fully understand that there are legitimate uses of Internet filtering but there can also be illegitimate uses of the practice. As you well know, in recent months the practice of Internet filtering has generated considerable attention among federal and state regulators and legislators as well as consumer groups, the general public and the media.

Therefore, I am submitting the enclosed shareholder proposal for inclusion in the 2008 proxy statement, in accordance with Rule 14a-8 of the General Rules and Regulations of the Securities Exchange Act of 1934. I am the beneficial owner, as defined in Rule 13d-3 of the Securities Exchange Act of 1934, of at least 200 shares of Verizon stock. I have held my shares continuously for more than one year and will be providing verification of my ownership. I will continue to hold all the shares through the next stockholders' meeting. My representative or I will attend the shareholders' meeting to move the resolution as required by the SEC rules. Thank you.

Sincerely,



Paul Haible

Encl.

**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 21<sup>st</sup> 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;
- 53% of Americans are uncomfortable with companies using their email content or browsing history to send relevant ads;
- 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 come under public scrutiny by consumer and civil liberties groups, regulatory authorities and shareholders.
- 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.



Trillium Asset Management Corporation  
[www.trilliuminvest.com](http://www.trilliuminvest.com)

November 14, 2008

Marianne Drost  
Senior Vice President  
Deputy General Counsel and Corporate Secretary  
Verizon Communications, Inc.  
1 Verizon Way  
Basking Ridge, NJ 07920

*Overnight Mail*

Dear Ms. Drost:

Trillium Asset Management Corporation ("Trillium") is an investment firm based in Boston specializing in socially responsible asset management.

I am authorized to notify you of our intention to file the enclosed shareholder resolution. Trillium submits this resolution 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. Trillium submits this proposal on behalf of our clients, who are the beneficial owners, per Rule 14a-8, of more than \$2,000 worth of Verizon Communications, Inc. common stock acquired more than one year prior to this date. Trillium is authorized to file this proposal and to represent our client's in this matter. They have stated their intention to hold this position throughout the date of the next annual stockholder meeting in 2009. We will provide verification of ownership from our custodian separately upon request. We will send a representative to the stockholders' meeting to move the resolution as required by the SEC rules.

I can be reached at (971) 222-3366 and look forward to your response.

Sincerely,

Jonas Kron, J.D., M.S.E.I.  
Senior Social Research Analyst

cc: Ivan G. Seidenberg, Chairman and Chief Executive Officer  
Ron Lataille, Senior Vice President, Investor Relations

BOSTON	DURHAM	SAN FRANCISCO	BOISE
111 Atlantic Avenue Boston, Massachusetts 02111-2809 T: 617-423-6655 F: 617-422-6179 800-548-5684	153 West Main Street, Second Floor Durham, North Carolina 27701-3215 T: 919-689-1265 F: 919-688-1451 300-853-1311	189 Pine Street, Suite 711 San Francisco, California 94104-3510 T: 415-392-4906 F: 415-392-4535 300-933-4806	910 W. Bannock Street, Suite 510 Boise, Idaho 83702-6118 T: 208-337-0777 F: 208-487-0278 300-567-0538

**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 21<sup>st</sup> 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;
- 53% of Americans are uncomfortable with companies using their email content or browsing history to send relevant ads;
- 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 come under public scrutiny by consumer and civil liberties groups, regulatory authorities and shareholders.

- 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.

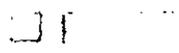
Therefore, be it resolved, that shareholders request the board issue a report by October 2009, excluding proprietary and confidential information, examining the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's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

Enter Your Location

All Verizon



Residential

Wireless

Small Business

Medium Business

Enterprise



## Privacy and Customer Security Policies

### Other Privacy & Policy Links

- [Internet Privacy Policy](#)
- [Letter from the CEO](#)
- [General Privacy Principles](#)
- [Telephone Company Customer Privacy](#)
- [FIOS TV Subscriber Privacy Notice](#)
- [Do Not Call Policy](#)
- [Browser Policy Statement](#)
- [Linking Policy Statement](#)
- [Terms and Conditions](#)
- [Your California Privacy Rights](#)
- [Ohio Telephone Customer Rights and Responsibilities](#)

### Letter from the Chief Executive Officer

Technology is changing the way all companies do business -- and changing the way they collect and use information about customers. Used responsibly, that information can help companies serve customers better. But, advances in communications technology bring growing concerns -- by customers and policymakers -- about maintaining the privacy of individual customer information.

We take privacy concerns very seriously. GTE and Bell Atlantic were built on more than a century of customer service and trust, and we work hard to continue that tradition. Our Companies have been guided by strong codes governing the privacy of customer communications and information. We have worked hard to establish Privacy Principles for Verizon that are the best in the industry.

These Privacy Principles embody our commitment and define our policy on safeguarding customer privacy. These principles strike a reasonable balance of customer concerns about privacy with their interest in receiving quality service and useful new products. This is especially important at a time when emerging telecommunications services present us with new business opportunities and new challenges to protecting customer privacy.

We recognize that our customers may have varying concerns regarding the information we obtain about them. Our Privacy Principles give our customers choice and flexibility regarding how we use that information. And these Principles guide our employees in handling customer information so that private information remains private.

At Verizon, we're committed to safeguarding customer privacy. We require our employees, partners and suppliers to protect the privacy of information about our customers. We're putting customers first -- and that's the key to Verizon's success in this dynamic marketplace.

Ivan Seidenberg, CEO

Updated January 2003

[About Us](#) | [Contact Us](#) | [Store Locator](#) | [Careers](#) | [Verizon Foundation](#) | [Site Map](#) | [Privacy Policy](#) | [Site Feedback](#) | [Terms and Conditions](#)

© 2008 Verizon

Español



Residential

Wireless

Small Business

Medium Business

Enterprise



## Privacy and Customer Security Policies

### Other Privacy & Policy Links

[Internet Privacy Policy](#)  
[Letter from the CEO](#)  
[General Privacy Principles](#)  
[Telephone Company Customer Privacy](#)  
[FiOS TV Subscriber Privacy Notice](#)  
[Do Not Call Policy](#)  
[Browser Policy Statement](#)  
[Linking Policy Statement](#)  
[Terms and Conditions](#)  
[Your California Privacy Rights](#)  
[Ohio Telephone Customer Rights and Responsibilities](#)

### General Privacy Principles

This tells you about the general privacy principles that guide all Verizon companies. Read more information about our [Internet Privacy Policy](#) and [Telephone Company Customer Privacy Policy](#).

1. Verizon obtains and uses individual customer information for business purposes only.
2. Verizon informs customers how information Verizon obtains about them is used, as well as their options regarding its use.
3. Verizon gives customers opportunities to control how and if Verizon uses individual information about them to sell them products and services.
4. Verizon enables customers to control how and if Verizon discloses individual information about them to other persons or entities, except as required by law or to protect the safety of customers, employees or property.
5. Verizon strives to ensure that the information we obtain and use about customers is accurate.
6. Verizon considers privacy implications as new services are planned and introduced and informs customers of the privacy implications of these services.
7. All Verizon employees are responsible for safeguarding individual customer communications and information.
8. Verizon participates in and supports consumer, government and industry efforts to identify and resolve privacy issues.
9. Verizon complies with all applicable privacy laws and regulations wherever Verizon does business.
10. Each Verizon company is responsible for implementing these Principles and informing customers about its privacy practices. Verizon encourages companies related to, but not wholly owned by, Verizon to adopt these Principles.

### Explaining the Guidelines

These ten Principles express Verizon's commitment to assuring strong and meaningful customer privacy protection in an era of rapidly changing communications technology and applications. The Principles are guidelines to help us work with our customers to properly use individual information acquired through a variety of lines of businesses. The goal is simple: balance our customers' concerns about privacy with their interest in receiving quality service and useful new products.

The Principles are based on the concepts of notice, choice and control. Verizon is committed to informing customers, and giving customers choices, about how we use information about them. Above all, the Principles are designed to ensure that Verizon will respect a customer's desire for privacy.

These Principles apply to our use of "individual customer information," that is, information about specific customers. Information that does not reveal a customer's identity is not individual customer information. For example, "aggregated information," such as the number of customers who have purchased Call Waiting in a particular state, or the number of users to access a Web site in a particular day, does not raise privacy concerns and is not covered by these Principles.

Under each Principle, we provide an explanation and list examples to give our employees and customers a sense of how these Principles are applied. The examples are intended to be illustrative, not all inclusive. Additional information about our privacy policy is available at our Verizon Web sites.

[Back to Top](#)

## Information Collection and Use

### Principle 1:

Verizon obtains and uses individual customer information for business purposes only.

We obtain information about our customers that helps to provide them with Verizon services. This information may also be used to protect customers, employees and property against fraud, theft or abuse; to conduct industry or consumer surveys; and to maintain good customer relations.

We may ask customers questions to better serve their special needs and interests. For example, our telephone company may ask whether customers work at home, whether any members of the household have special needs, or whether teenagers reside in the household, in order to determine whether customers may be interested in additional lines, ISDN or other services.

Access to databases containing customer information is limited to employees who need it to perform their jobs – and they follow strict rules when handling that information.

[Back to Top](#)

### Principle 2:

Verizon informs customers how information Verizon obtains about them is used, as well as their options regarding its use.

Verizon discloses to customers the types of information a Verizon business unit obtains about customers, how and when it is used, when it might be disclosed, the stringent measures we employ to protect it, and ways the customer can restrict the use or disclosure of that information.

For customers of our online services, we will disclose how individual customer information is obtained (whether through customer registration or through automatic means), what kind of information is obtained, and the purpose for which we use the information obtained on line.

Customers may obtain information regarding Verizon's privacy policy by accessing our World Wide Web site at <http://www.verizon.com>, or by requesting information from a Verizon service representative.

[Back to Top](#)

### Principle 3:

Verizon gives customers opportunities to control how and if Verizon uses individual information about them to sell them products and services.

Customers have many opportunities to control how we use their individual information to introduce them to new products and services. For example, Verizon will not call customers who have expressed to us a preference not to be called for marketing purposes. Customers can also have their names removed from direct mail lists that we use. The same will be true for email; if any Verizon business unit decides to use email to send new product information to its customers.

However, we do use individual customer information internally for our own general marketing and planning purposes -- so that we can, for example, develop, test and market new products and services that meet the needs of our customers. Ordinarily, such information is combined into aggregations that do not include individual customer identities. Under certain circumstances, we are required by law to disclose the aggregated information to other companies, but in such cases customer identities are not included.

[Back to Top](#)

## Disclosure of Individual Customer Information

### Principle 4:

Verizon enables customers to control how and if Verizon discloses individual information about them to other persons or entities, except as required by law or to protect the safety of customers, employees or property.

Subject to legal and safety exceptions, Verizon will share individual customer information only with persons or entities outside the company when the customer has consented, or when we have advised the customer of the opportunity to "opt-out" (to choose not to have the information disclosed).

If Verizon enters into a merger, acquisition, or sale of all or a portion of its assets, a customer's personally

identifiable information will, in most instances, be transferred as a part of the transaction.

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

An example of when Verizon would disclose individual customer information to an outside entity is when Verizon is served with valid legal process for customer information. In such cases, we are required to release the information. We are also required by law to provide billing name and address information to a customer's long distance carrier and other telephone companies to allow them to bill for telecommunications services. (By law, customers with non-published or unlisted service have the right not to have their billing name and address disclosed when they make a calling card call or accept a collect or third party call. However, if they do restrict disclosure, they will be unable to make calling card calls or accept collect and third party calls.)

Similarly, we are required to provide directory publishers with listings information -- name, address and phone number -- for purposes of publishing and delivering directories. In addition, under certain circumstances, our telephone company shares customer information with other carriers and with law enforcement to prevent and investigate fraud and other unlawful use of communications services.

[Back to Top](#)

## **Accuracy of Individual Customer Information**

### **Principle 5:**

Verizon strives to ensure that the information we obtain and use about customers is accurate.

Verizon is committed to ensuring that the information we obtain and use about customers is accurate. To that end, we strive to verify that our customer records are correct. Customers who find an error in their Verizon bills are encouraged to notify Verizon. Verizon's service representatives are trained to answer customer questions about, and to give customers reasonable access to, the information we have about them. Our service representatives will also provide explanations of how such information is used and how to correct any inaccuracies if they occur.

[Back to Top](#)

## **Privacy and Verizon Services**

### **Principle 6:**

Verizon considers privacy implications as new services are planned and introduced and informs customers of the privacy implications of these services.

Verizon offers several privacy-enhancing services, including Non-Published numbers, Caller ID, Caller ID With Name, Per Call Blocking, and Anonymous Call Rejection. We also work to develop other services that help customers to control access to information about them. We seek customer input in developing new products and conduct comprehensive customer outreach and education before and after introducing privacy-sensitive products. We take these steps in accordance with these Privacy Principles as well as our Universal Design Principles, which govern the accessibility of our services to the broadest possible range of diverse users.

At Verizon, we are committed to expanding the world of communications and multimedia for customers -- a world of wireline and wire-free solutions...voice, video and data services...information and entertainment. We will investigate the privacy implications these new services may have and build safeguards into services before they are introduced. We will inform and educate customers about the effect on privacy the new services may have.

[Back to Top](#)

## **Information Management and Security**

### **Principle 7:**

All Verizon employees are responsible for safeguarding individual customer communications and information.

Verizon's Employee Code of Business Conduct, which is distributed to all employees, requires Verizon personnel to be aware of and protect the privacy of all forms of customer communications -- whether they are voice, data or image transmissions -- as well as individual customer records. The Code makes clear

that employees who fail to follow the Privacy Principles will face disciplinary action, which can include dismissal. All employees are trained regarding their responsibilities to safeguard customer privacy.

We strive to ensure that information we have about our customers is accurate, secure and confidential, and to ensure that our employees comply with our privacy policy. We never tamper with, intrude upon or disclose the existence or contents of any communication or transmission, except as required by law or the proper management of our network. Access to databases containing customer information is limited to employees who need it to perform their jobs -- and they follow strict guidelines when handling that information. We use safeguards to increase data accuracy and to identify and authenticate the sources of customer information. We use locks and physical security measures, sign-on and password control procedures, and internal auditing techniques to protect against unauthorized use of terminals and entry into our data systems.

Verizon requires that records be safeguarded from loss, theft, unauthorized disclosure, and accidental destruction. In addition, sensitive, confidential, or proprietary records must be protected and maintained in a secure environment. It is our policy to destroy records containing sensitive, confidential, or proprietary information in a secure manner. Hard copy confidential, proprietary, or sensitive documents must be made unreadable before disposition or recycling, and electronic media must be destroyed using methods that prevent access to information stored in that type of media. Just as employees would report stolen property, missing records and suspicious incidents involving records are referred to Verizon Security.

We encourage our employees to be proactive in implementing and enforcing the Verizon's privacy policies. If employees become aware of practices that raise privacy concerns, they are encouraged to report them to their supervisors or to contact Verizon's Ethics or Security office.

[Back to Top](#)

## **Compliance With Laws and Public Policy Participation**

### **Principle 8:**

Verizon participates in and supports consumer, government and industry efforts to identify and resolve privacy issues.

We participate in legislative and regulatory proceedings, industry association efforts, consumer group efforts, and general business group activities relating to telecommunications privacy issues. Our External Affairs department is responsible for coordination of Verizon's public policy participation.

We believe that developing international privacy protection and information-use standards is necessary to protect the needs of our customers. Verizon supports the development of international standards to protect individual customer information and its proper use on a worldwide basis.

[Back to Top](#)

### **Principle 9:**

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

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

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

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

[Back to Top](#)

## **Implementation**

### **Principle 10:**

Each Verizon company is responsible for implementing these Principles and informing customers about its privacy practices. Verizon encourages companies related to, but not wholly owned by, Verizon to adopt these Principles.

Every Verizon business unit is responsible for:

- Evaluating its particular needs and determining how to implement the Principles;
- Developing its own privacy policies and procedures based on the Principles, and developing additional privacy policies and procedures if needed;
- Informing its employees of the policies and training them in the proper procedures; and
- Informing customers how personal customer information is used and how they can control its use and disclosure.

Verizon's Corporate Compliance Officer is responsible for ensuring that all Verizon business units and their employees comply with privacy laws and regulations.

Verizon requires any vendors and consultants we hire, as well as suppliers and contractors, to observe these privacy rules with respect to any of our customers' individual customer information. They must abide by the Principles when conducting work for us, and they will be held accountable for their actions.

[Back to Top](#)

Updated November 2005

[About Us](#) | [Contact Us](#) | [Store Locator](#) | [Careers](#) | [Verizon Foundation](#) | [Site Map](#) | [Privacy Policy](#) | [Site Feedback](#) | [Terms and Conditions](#)

© 2008 Verizon

[Español](#)

Enter Your Location

All Verizon



Residential

Wireless

Small Business

Medium Business

Enterprise



## Privacy and Customer Security Policies

### Other Privacy & Policy Links

[Internet Privacy Policy](#)  
[Letter from the CEO](#)  
[General Privacy Principles](#)  
[Telephone Company Customer Privacy](#)  
[FiOS TV Subscriber Privacy Notice](#)  
[Do Not Call Policy](#)  
[Browser Policy Statement](#)  
[Linking Policy Statement](#)  
[Terms and Conditions](#)  
[Your California Privacy Rights](#)  
[Ohio Telephone Customer Rights and Responsibilities](#)

### Internet Privacy Policy

As always, the privacy and security of your personal information is our #1 priority, and we want you to be aware of how we collect and handle information on our site.

When you visit verizon.com, we may collect the following information about your visit:

- Anonymous statistics collected as you browse the site
- Personal information you knowingly give us



For details about our general and Internet privacy policies, you may select from the topics to the left or search our privacy FAQs below:

#### Please select a question

What does it mean to me for Verizon to be a licensee of the TRUSTe Privacy Program?



#### What does it mean to me for Verizon to be a licensee of the TRUSTe Privacy Program?

The TRUSTe seal confirms that Verizon is a licensee of the TRUSTe Privacy Program. Verizon wants you to feel confident about your privacy when using verizon.com, so we have TRUSTe review this site for compliance with their guidelines. TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. Contact us if you have questions or concerns regarding this statement. If your inquiry has not been satisfactorily addressed, you should then contact TRUSTe who will serve as a liaison to resolve your concerns.

[Back to Top](#)

### Information Verizon Collects

#### What information does this Web site gather?

Verizon collects personal information such as name, address, and email address, when you knowingly provide it to us. In addition, Verizon may collect other information provided by you, such as your credit card number, billing address, Social Security Number (SSN) and date of birth, when you set up an online account or order service online. Our Web servers automatically collect statistical information about your visit such as pages visited and which browsers are used to visit our site. None of this information is associated with you as an individual (see information about cookies). We use these statistics to monitor our site's performance and to make it easier for you to use.

If you choose to use an available referral service to tell a friend about our site or a specific product or service, we will ask for your friend's name and email address. We will then send your friend a one-time email regarding our site or the featured product or service. Verizon uses this information for purposes of sending this one-time email and tracking the success of the referral service.

[Back to Top](#)

#### What happens when I provide personal information on this Web site?

When you supply information for a specific purpose, such as online ordering of a Verizon service, we use the information for that purpose.

When you use our Web site to order services, we may use this individually identifiable information as we would if obtained in a non-electronic manner. Such information may include:

- Publishing your name, address, and phone number in our directories (unless you have requested a non-published or non-listed number)
- Evaluating your service needs and contacting you regarding additional services you may find useful

If the way we use personally identifiable information changes, Verizon will contact you via email notifying you of this change and giving you the opportunity to opt out of such use.

[Back to Top](#)

#### **What happens when I provide information on registration forms?**

When you choose to register with [verizon.com](#) or any other Verizon site, we request accurate contact information and preferences that help us better serve you. You will always retain the option to choose if your contact information is used to send you company and product information, special offers, and in some cases, newsletters.

If you're a local Verizon phone service customer, you may be given the option to register a profile with us (limited to specific areas). We would then store your name, purchase history, and billing information to make it easier for you to shop and purchase from us in the future. Customers have access to their account information on their monthly bills or by establishing an account online.

At anytime you may:

- Elect not to receive (opt out) marketing email messages. The primary purpose of these messages is the commercial advertisement or promotion of a Verizon product or service. At any time after the initial registration, you can opt out by selecting the opt-out cancel option in your profile within the application itself.
- Update your contact and personal information anytime by updating your account and/or your profile (where available) within the application.

In order to improve your experience with us, we may decide to improve our site's ability to obtain information about users. We will update this privacy statement continually to ensure that you are aware of developments in this area.

[Back to Top](#)

#### **Does Verizon sell or give my information to non-Verizon companies?**

No. We do not sell or disclose individually identifiable information obtained online about our visitors to anyone outside of Verizon. The only exceptions to this rule are the following:

- If you specifically authorize Verizon to share your information with another company
- It is required by law and when we believe that disclosure is necessary to protect our rights and/or to comply with a judicial proceeding, court order, or legal process served on our Web site
- Disclosure is necessary to protect the safety of customers, employees, or property
- Publishing your name, address, and phone number in our directories if you initiate your telephone service with us online (unless you have requested a non-published or non-listed number)
- Sharing data with our authorized vendors, contractors and agents, only to the extent necessary for them to perform their work, in order that Verizon can carry out certain functions in marketing and delivering services to you.

If you provide individually identifiable information at an event Verizon sponsors with another company, or if you register on a co-sponsored Web site, or if you have elected to participate in an affinity program (such as airline miles), you may be providing the individually identifiable information to the co-sponsor as well as Verizon. Review the privacy statement at the event or on the co-branded site or the affinity site to learn how the partner uses this information. Be assured that Verizon uses this information in accordance with this privacy policy.

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

[Back to Top](#)

#### **Does Verizon accommodate links to other sites?**

Yes. Our site contains links to other Web sites. We are not responsible for the content or the privacy

practices employed by other sites. However, in some instances where a service is provided through a non-Verizon partner or supplier site, such as Online Bill Pay, you can feel confident that your individually identifiable information will be protected. Verizon requires suppliers not to use the information for any purpose other than the purpose for which it was originally collected, protecting the privacy of your information.

[Back to Top](#)

**What does Verizon do with non-personally identifiable information collected automatically?**

Verizon uses cookies to collect this type of information in order to enhance your online experience as follows:

- Ensure that you see the correct products and pricing applicable to the state in which you live
- Manage the number of ads that you see to avoid over-delivery of the same message
- Tailor an advertisement to better match your interests and preferences

[Back to Top](#)

**What does Verizon do with personally identifiable information?**

Personal information you voluntarily supply when obtaining information, purchasing products, or interacting with our advertising on verizon.com **is not shared** for non-Verizon purposes. This information is Verizon proprietary data and is not available for use to any outside company in this personalized form. Should any changes be made in the way we use personally identifiable information, Verizon will contact you via email notifying you of this change and give you the opportunity to choose to opt out of such use.

[Back to Top](#)

**Does Verizon use the information provided online to profile its customers?**

No. Verizon does not combine offline information about you with the online information that you provide on our Web site.

We have made it a requirement that you will be clearly notified at the time of online data collection for the purpose of consumer profiling. When your online purchase behavior is intended to be combined with offline information, this intent will be clearly stated. You will then have the ability to choose not to have that information combined.

[Back to Top](#)

## **Email**

**Does this site send email to site visitors?**

Verizon strives to continuously improve our customers' online experience by providing them with the latest information about the benefits of Verizon's products and services and in other circumstances described below. We may provide this information in any number of ways, including emails to our customers, online visitors and others who have provided their email addresses to Verizon. In addition, unless you have chosen to opt out from receiving email messages from Verizon, Verizon may send emails to:

- Inform customers that their telephone bills are available for review online
- Conduct online surveys
- Provide marketing information about Verizon products and services
- Provide information to those who have voluntarily provided their email addresses to third parties in order to receive promotional material

Moreover, in the following situations, Verizon reserves the right to communicate through email with online users, including those who have opted out of receiving solicitation-based emails, to:

- Notify customers about service or product affecting changes
- Respond to an online user's email
- Confirm transactions, orders, payments and registrations placed online
- Send information that a customer or potential customer has requested
- Provide emergency, security and online account maintenance information

Verizon supports and complies with all laws governing its email communications and will update this policy as needed to ensure ongoing compliance.

[Back to Top](#)

## Security Issues

### How does Verizon protect my personal information?

We are committed to protecting the information you give us, so we implement the appropriate safeguards to do so. Any information that you give us is protected by a password with a minimum of six characters for added security. Within Verizon, your information is stored in password-protected, limited-access servers. Wherever possible, Verizon servers reside behind a corporate firewall that maintains tight controls on any access to the system from both our internal network and the Internet. Verizon uses Secure Socket Layer (SSL) to transmit sensitive information such as credit card numbers and SSN. SSL is a transport level technology for authentication and data encryption between a Web server and a Web browser. SSL sends data over the "socket" which is a secure channel at the connection layer.

### Does Verizon's Web site collect information from children?

Verizon believes that protecting the privacy of children on the Internet is very important. The Verizon Web site is not designed to attract children under the age of 13, and we do not intentionally collect personal information from children on our Web sites. Ordering online products and services is limited to adults 18 or over.

Children should exercise caution before providing personal information online and should discuss with an adult or guardian before doing so. Verizon also urges parents and guardians to consider using one of the low-cost software programs designed to protect children while they are online.

[Back to Top](#)

## Cookies

### What are cookies and why does Verizon use them?

A cookie is a small data string our server writes to your hard drive. This data string contains your unique user ID for our Web site. This technology also allows us to customize your experiences when you visit the Verizon Web site. For example, we're able to deliver content specific to your interests, keep track of your online ordering and alert you to new products or money saving opportunities based on your current services.

[Back to Top](#)

### What information is collected by the site or in cookies?

Verizon collects non-personally identifiable information regarding your visit, usually in the form of cookies, log files, or clear .gif files. Cookies contain a session identification number that our systems use to recall previous authentication or order information from our servers. We may also collect your domain name, IP address, the address of the last URL you visited prior to coming to our Web site, and your browser and platform type. We use third party tracking services to help us analyze this information in the aggregate to evaluate the effectiveness of our site. In some cases, the information is collected directly by the third party and in others it is forwarded by Verizon to the third party. The third party is not permitted to use the information for any other purpose.

[Back to Top](#)

### How do I disable cookies on my browser?

It's important you know that a cookie cannot be used to access or otherwise compromise the data on your hard drive. Your privacy is always protected. However, at any time you may choose to change your browser settings to disable cookies if you do not want us to establish and maintain a unique verizon.com user ID for you. Please be aware that cookies may be required to complete certain functions on this Web site, such as ordering online. We've made it easy for you to remove cookies from your browser. Simply choose from the list below and click on the name of the browser you use to access the Internet to find instructions.

#### PC Users

[Microsoft® Internet Explorer 6.x](#)  
[Microsoft Internet Explorer 5.x](#)  
[Netscape® 7.x](#)  
[Netscape 6.x](#)  
[Mozilla Firefox™ 1.x](#)

#### Macintosh® Users

[Netscape 7.x](#)  
[Safari 1.x](#)

[Back to Top](#)

## Online Advertising

### What is Verizon's position regarding online advertising and third-party ad servers?

As an online advertiser, Verizon uses information supplied from third-party companies in several ways. This is aggregated data that does not personally identify any individual online user. This data is used to:

- Evaluate and prioritize site selection when developing online media plans
- Geographically target advertising
- Deliver product and pricing information applicable to the customer's state
- Gauge the effectiveness of our online advertising

Again, personally identifiable information such as name, address, phone number, or email address is not collected unless you voluntarily supply this data to Verizon or to a third party partner in order to get further information about Verizon products and services.

In addition, some Verizon Web sites -- for example, [www.SuperPages.com](http://www.SuperPages.com) -- may accept advertisements from third-party advertisers. These advertisers are carefully selected to provide information about products and services that we think may benefit you. Please check the privacy policy of these Web sites concerning what information may be collected by third-party advertisers.

Third-party advertising companies may also utilize technology in order to measure the effectiveness of ads. Some Verizon Web pages contain clear .gif files (also known as Web beacons), electronic images that allow the third party to collect anonymous information. This anonymous information about your visits to our site is used to provide advertisements about goods and services of potential interest to you. No personally identifiable information is collected during this process.

[Back to Top](#)

### Whom do I contact if I am concerned, or have questions, about my Privacy at Verizon?

Please visit [Contact Us](#).

[Back to Top](#)

Updated January 2006

[About Us](#) | [Contact Us](#) | [Store Locator](#) | [Careers](#) | [Verizon Foundation](#) | [Site Map](#) | [Privacy Policy](#) | [Site Feedback](#) | [Terms and Conditions](#)

© 2008 Verizon

[Español](#)

# Guiding Principles for Content on Verizon Networks



**Our goal is simple . . .  
to help you access the  
content you want and  
avoid content you don't.**

Verizon builds great networks—broadband, mobile and global. These networks allow us to deliver communications, data and entertainment content to our customers in an array of ways that few companies can—through FiOS TV, Verizon Online and Verizon Wireless mobile devices.



As one of the world's leading communications providers, Verizon believes in open networks and that network operators should provide access to all lawful content on the Internet.

We also believe it is important for our customers to have access to the tools they need to choose and manage what content they and their families wish to receive.

We have adopted Content Guidelines based on these core principles. These guidelines will help us make content decisions consistent with our values—respect for customer choice, privacy and safety. By applying them, we can help make our customers' lives richer and their experience with Verizon's services more enjoyable, productive and meaningful.

#### **VERIZON'S GUIDING PRINCIPLES FOR CONTENT**

- Where Verizon offers its own content, or other parties' content through one of its platforms such as V CAST or Verizon Surround, it does so based on factors that include content ratings provided by existing rating systems and consistency with acceptable industry practices.

Verizon believes in empowering customers to make informed choices about the content they seek to access by providing customers with available ratings information and parental controls.

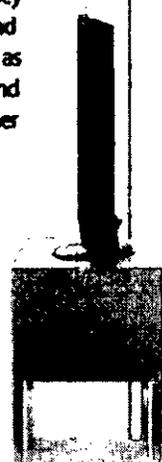
- As a network provider, Verizon provides access to the Internet and, through it, to services and content that Verizon does not own, develop or control.

Verizon is committed to helping its customers make informed decisions about the content they want to access over Verizon's network and will provide content management tools, as well as access to educational materials and other resources to assist parents and other users in identifying content they deem appropriate.

- Verizon respects freedom of expression and our customers' ability to freely access and disseminate lawful content of their choosing in a manner that respects others' use of the network and that complies with the law.

Verizon supports sound industry practices for safeguarding children, intellectual property rights and our customers' privacy and security.

- Verizon exercises broad discretion over its choice of brands and companies that advertise on its platforms. In selecting advertising partners and content, Verizon takes into account its corporate values, as well as the values of our business partners and customers.



## Verizon's Content

We hold ourselves to high standards for content that Verizon produces, or others produce on our behalf, such as some programming distributed on VCAST, FiOS One TV and Verizon Surround.

We will not knowingly distribute such content if it:

- contains material that is obscene, is indecent, has strong sexual, explicit or erotic themes, or has links to such content; or
- contains hate speech; or
- contains excessive violence; or
- contains extreme profanity; or
- contains misleading or fraudulent claims; or
- promotes or glamorizes alcohol abuse, illegal drug use or the use of tobacco products.

## Third-Party Content That Verizon Distributes

We present different kinds of content on Verizon-branded wireless, Internet and TV platforms. Programming runs the gamut from news, weather, and sports programs to movies, music, and videos available for download.

When we assess what standards should apply to this third-party generated content, Verizon distinguishes between rated and un-rated content. When content has been rated, the parental controls we provide and content management tools we offer enable customers to limit or restrict access to it. What's more, FiOS TV customers can even block all un-rated content if they wish.

Empowering our customers is why we strongly encourage content providers to have their programming, games, music or other types of content rated by third-party rating organizations. If content is not rated, we will not offer it on a Verizon-branded platform unless it complies with the same requirements we place on our own content.

## Short Code-Based Messaging Campaigns

The use of short code-based messaging varies widely. Short code campaigns that distribute content such as wallpapers or ringtones, that advertise or market companies, goods or services or provide user-generated content services must comply with our guidelines for such campaigns. For other uses, including campaigns of political and advocacy groups, Verizon Wireless will provide short code-based messaging services to any group delivering legal content to customers who affirmatively indicate they wish to receive it.

All short code-based messaging campaigns must also comply with applicable industry standards.\*

## Content to Which Verizon Provides Access

As Internet access providers, Verizon Online and Verizon Wireless enable customers to access content, on web sites and newsgroups, which Verizon does not generate, own or control.

The Internet is a free marketplace of ideas, with content of limitless variety for a very broad range of individual tastes.

At Verizon, we believe you can best choose what content is appropriate for you and your family, so each Verizon network provides access to content management tools such as parental controls — to help you control what is accessible to Internet users in your home.

## User-Generated Content

Verizon applies guidelines to services that let users post, transmit or generate their own content — such as chat programs, blogs, social networks, and photo or video portals.

Under these guidelines, applications that appear on a Verizon platform such as Mobile Web or Verizon Surround must not only comply with the law, but also adhere to a set of sound practices with safeguards to protect users against abuse, fraud and other inappropriate conduct or activities. These safeguards should, in particular, protect children and adolescents from predators and inappropriate content.

Third parties hosting these user-generated content services should also adopt their own policies and practices to ensure compliance with the law, including appropriate notice and take-down procedures for unlawful content.

## Advertising Content

All advertising which appears on Verizon-branded platforms must not only comply with the law, but also with applicable industry standards\* established by groups such as the Mobile Marketing Association's Best Practices, the Child Advertising Review Unit and CTIA's Consumer Code.

Verizon has broad discretion over the advertisements that will run over its services. We may reject advertising for several reasons, including failing to comply with Verizon's standards of decency or good taste; being misleading or inaccurate; or making fraudulent or unfair competitive claims. We may also reject advertising promoting our competitors, or that may harm Verizon's brand or public image.



\* For links to information about industry standards, see [Link Here](#)





### Note to Reader:

This summary is designed to share with our customers, business partners and others how Verizon views and approaches important policy issues involving content. It discusses how ratings, parental controls and other content management tools can help our customers select the content they and their families may access using Verizon's networks and services and how they may choose to restrict access to unwanted content.

This brochure informally describes the principles which guide Verizon's policy and decision-making regarding content available through our networks. It is not a substitute for Verizon's complete policies and practices pertaining to content. It does not attempt to define all requirements applicable to content or to define the legal rights or obligations of our customers, our business partners or Verizon. This brochure is not intended to constitute a contract, and Verizon's content policy may change from time to time to address changes in the marketplace and consumer expectations.

To download full copies of Verizon's Content Policies, visit:  
**[verizon.com/contentpolicy](http://verizon.com/contentpolicy)**

#### FOR INFORMATION ABOUT INDUSTRY STANDARDS, VISIT:

CTIA CONSUMER CODE:

**[www.ctia.org/content/index.cfm/AID/10352](http://www.ctia.org/content/index.cfm/AID/10352)**

CTIA CONTENT GUIDELINES:

**[www.ctia.org/advocacy/policy\\_topics/topic.cfm/TID/36](http://www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36)**

MOBILE MARKETING ASSOCIATION'S BEST PRACTICES:

**[www.mmaglobal.com/bestpractices.pdf](http://www.mmaglobal.com/bestpractices.pdf)**

CHILDREN'S ADVERTISING REVIEW UNIT  
OF THE COUNCIL OF BETTER BUSINESS BUREAUS.

**[www.caru.org/guidelines](http://www.caru.org/guidelines)**

Verizon Communications Inc. (NYSE: VZ), headquartered in New York, is a leader in delivering broadband and other wireline and wireless communication innovations to mass market, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, serving nearly 66 million customers nationwide.

A Dow 30 company, Verizon employs a diverse workforce of nearly 235,000 and in 2007 generated consolidated operating revenues of \$93.5 billion.

For more information about Verizon, please visit:  
**[verizon.com](http://verizon.com)**

**verizon**

# Content Policy for Verizon Networks



## Contents

■ Guiding Principles	3
■ FiOS TV Guidelines	4
■ Verizon Online Guidelines	7
■ Verizon Wireless Guidelines	9
■ Wireless Short Code Guidelines	11
■ Verizon Business Guidelines	11
■ User Generated Content Guidelines	12
■ Advertising Guidelines	14

### Note to Reader:

The guidelines that follow describe Verizon's policies and practices with respect to the various types of content that we make available to our customers through Verizon's wireless, Internet and television services, and the policy issues that relate to such content.

These guidelines offer our customers, business partners and others interested in Verizon's views on content management insight into how we at Verizon view and approach the important policy issues involving content. The guidelines address the use of ratings and other standards, and the use and availability of parental controls and other means we make available to help our customers control the content that they and their families can access and view over Verizon's network.

It is important to note that while these guidelines describe our policies with respect to content that Verizon develops or presents under the Verizon brand, or content that we do not control that is available to our customers through our various services, they are not intended to constitute a contract or to define all operational or commercial requirements applicable to such content. Nor are these guidelines intended to define the legal rights or obligations of our customers or Verizon, as they may change from time to time.

## Verizon's Guiding Principles for Content

Verizon distributes, produces and facilitates access to content in a manner consistent with its corporate values. These values include respect for customer choice, respect for customer privacy and security, and dedication to full compliance with the law.

Accordingly, Verizon adheres to the following Guiding Principles with respect to content:

1. Where Verizon offers its own content or other parties' content through one of its platforms, it does so based on factors that include content ratings provided by existing rating systems and consistency with acceptable industry practices. Verizon believes in giving customers the ability to make informed choices about the content it offers by making any ratings and other information readily available to customers and by giving customers access to the tools they can use to monitor and control the content they obtain.
2. As a network provider, Verizon provides access to the Internet and, through it, to services and content, the substance of which, Verizon does not own, develop or control. Verizon is committed to empowering its customers to make informed choices about the services and content they want to access over its network. Verizon is committed to supporting its customers by providing access to personal content management tools, such as parental controls, as well as access to educational materials and other resources about content rating systems to assist parents and other users in identifying appropriate content for themselves and their children.
3. Verizon respects freedom of expression and our customers' ability to freely access and disseminate the lawful content of their choosing in a manner that respects others' use of the network and that complies with the law. Verizon supports sound industry practices for safeguarding children, the intellectual property rights of content owners, and the privacy and security of our customers.
4. Verizon exercises broad discretion over its choice of brands and companies that advertise on its platforms. Verizon's selection of advertising partners and content takes into account our corporate values as well as those of our business partners and customers.

## Verizon FiOS TV's General Content Guidelines

### 1. Content Generated By Or On Behalf of Verizon FiOS TV:

This category covers content/programming that FiOS TV generates or produces, or to content that a third party generates or produces on FiOS TV's behalf. Content in this category is closely identified with the FiOS TV brand and FiOS TV generally has a higher degree of control over it. Examples of content in this category include programming on FiOS TV's FiOS One Channel such as the Push/Pause and Limbo television series.

A. Content standard for this category - FiOS TV will only air content in this category that is lawful and will not knowingly air content that includes material in any of the following excluded content categories:

- Content that contains anything that is obscene or indecent, or anything with strong sexual, explicit or erotic themes or that links to such content; or
- Content that contains hate speech; or
- Content that contains excessive violence; or
- Content that contains extreme profanity; or
- Content that contains misleading or fraudulent claims; or
- Content that promotes or glamorizes alcohol abuse, illegal drug use or use of tobacco products.

Consistent with prevailing industry standards, content that does not satisfy the above guidelines may be aired by FiOS TV if it is included in the context of artistic, educational, medical, news, scientific, or sports material.

### 2. Third-Party Content FiOS TV Distributes On The Verizon FiOS TV-Branded Video Programming Distribution System:

This category covers third-party programming FiOS TV licenses from other entities and distributes over Verizon's FiOS TV video programming distribution system. Examples of content in this category include the ESPN, Discovery Channel, CNN, ABC, CBS and NBC channels, as well as Hollywood movies and other individual programming assets. In contrast to the content in Category 1, above, content in this category is licensed from third parties and is distributed on the FiOS TV-branded platform without editorial control or input from FiOS TV management.

Much of the content in this category is rated by a third-party ratings body, and to the extent feasible, FiOS TV will leverage existing ratings systems and content management tools to empower customers to make their own choices about the types of content they choose to view. Parental controls are available for most, if not all, of this content.

Additionally, FiOS TV may, in its discretion and where it has the ability to do so, elect not to license a particular channel or distribute specific content that is inconsistent with Verizon's Guiding Principles on Content. For those channels that FiOS TV elects to distribute, FiOS TV has no editorial input or control over the specific programming aired by the channel.

The content standards for content in this category are described below:

- A. Content Standard for Rated Content - Third-party groups have rated this content and content management tools, such as parental controls and service blocks, are available to limit or restrict access to content.
- B. Content Standard for Content That Is Not Rated - Content in this category has not been rated. However, FiOS TV offers state-of-the-art content management tools, such as parental controls and service blocks that allow customers to block this content in its entirety. However, consistent with industry practice, parental controls may not restrict news, weather, and sports programming.
- C. Mature-Themed Programming Content - Content in this category is Not-Rated, and customers may block this content in its entirety by activating FiOS TV's state-of-the-art parental controls.

In all of the above cases, FiOS TV will only distribute content that is lawful and is consistent with similar types of programming offered by major cable and satellite providers.

**3. Content to Which FiOS TV, As A Video Programming Distributor, Is Required To Provide Access:**

Content in this category covers content that FiOS TV, in its role as a video programming distributor, is required, by law or regulation, to offer to customers, but which FiOS TV does not purchase, license, develop, generate, promote or exercise editorial control over. The content standards for content in this category are described below:

- A. Content Standard for Leased Access Channels - Content in this category refers to unaffiliated third-party programming contained on FiOS TV's leased access channels that FiOS TV is required to exhibit pursuant to Federal law and the Federal Communications Commission's Leased Access Rules (47 C.F.R. § 76.701). As a general matter, Federal law and regulation does not allow FiOS TV to have editorial control or input over content third parties air on the FiOS TV leased access channels.

However, consistent with Federal Law and the Federal Communications Commission's Leased Access rules (47 C.F.R. § 76.701), content on FiOS TV's Leased Access channels should not include obscenity, indecency, or nudity. Accordingly, FiOS TV has the right to reject any such content, and any third party that desires to air programming on the FiOS TV Leased Access channels must first, among other things, certify that such content is not obscene or indecent.

Content on Verizon's Leased Access channels is Not-Rated, and customers may block this content in its entirety by activating FiOS TV's state-of-the-art parental controls.

- B. **Content Standard for Public, Educational and Government (PEG) Channels -** Content in this category is unaffiliated third-party programming contained on FiOS TV's PEG channels that FiOS TV is required to exhibit pursuant to state and/or local franchise agreements. As a general matter, FiOS TV does not have editorial control or input over content contained on the PEG channels that are carried on FiOS TV. Pursuant to the Federal Communications Commission's PEG Channel rules (47 C.F.R. § 702), FiOS TV may refuse to transmit any public access program that Verizon reasonably believes contains obscenity. Content on Verizon's PEG channels is Not-Rated, and customers may block this content in its entirety by activating FiOS TV's state-of-the-art parental controls.
- C. **Content Standard for Web-based Programming -** Content in this category refers to unaffiliated third-party programming available via the Internet, which FiOS TV customers may be able to access using the FiOS TV set-top box and network. Content obtained from the Internet through FiOS TV is covered by, and subject to, Category 3 of the Verizon Online General Content Guidelines.

## Verizon Online's General Content Guidelines

### 1. Content Generated By Or On Behalf Of Verizon Online:

This category covers content that Verizon Online generates or produces or content that a third party generates or produces on Verizon Online's behalf. Content in this category is closely identified with Verizon or Verizon Online, and Verizon generally has a higher degree of control over it. Examples of content in this category include certain content appearing on Verizon Surround (like V CAST Today) and original content such as FiOS One episodes displayed on a Verizon Online platform.

A. Content standard for this category - Verizon Online will only distribute content that we produce or generate (or others do on our behalf) that is lawful and will not knowingly distribute content that includes material in any of the following excluded content categories:

- Content that contains anything that is obscene or indecent, or anything with strong sexual, explicit or erotic themes or that links to such content; or
- Content that contains hate speech; or
- Content that contains excessive violence; or
- Content that contains extreme profanity; or
- Content that contains misleading or fraudulent claims; or
- Content that promotes or glamorizes alcohol abuse, illegal drug use or use of tobacco products.

Consistent with prevailing online industry standards, content that does not satisfy the above guidelines may be distributed by Verizon Online if it is included in the context of artistic, educational, medical, news, scientific, or sports material.

### 2. Third-Party Content Verizon Online Distributes On A Verizon Online-Branded Distribution Platform:

This category covers content contained on a Verizon Online-branded distribution platform (e.g., Verizon Surround) but which is not created by or on behalf of Verizon Online. Examples include NFL Network, Music by Rhapsody, and other similar content.

The content standards for content in this category are described below:

A. Content Standard for Rated Content - "Rated content" refers to content that third-party groups have rated and for which content management tools, such as parental controls, are available. Verizon Online will typically require its content suppliers to provide their content with a rating that is benchmarked to the appropriate industry standard (e.g., Electronic Software Ratings Board, Recording Industry Association of America, Motion Picture Association of America.).

- B. **Content Standard for Content That is Not Rated** - Content in this category has not been rated by any third-party ratings group. In making this content available, Verizon Online will generally adhere to the guidelines in Category 1, above, and will not knowingly distribute content that does not adhere to these guidelines.

In each of the above cases, content appearing on Verizon Online-branded distribution platforms must be lawful and consistent with standard industry practices. In addition, Verizon (and others) makes available content management tools, such as parental controls, to help parents and other users limit access to content they may find objectionable.

- C. **Internet Search** - The use of Internet search tools can lead to content that some users may find unsuitable. Recognizing this, Verizon Online makes available safe search tools for searches conducted on Verizon-branded websites that help its customers determine the level of search filtering they deem appropriate, and that help parents and other users to limit access to content they may find objectionable.

**3. Content to Which Verizon Online, As A Network Provider, Provides Access:**

**General Internet Content:** This category covers non-Verizon content that customers access using their Internet connection. Content in this category includes the vast range of information and images generally available via the Internet through websites, search, newsgroups, and other sources. Verizon Online does not generate, own or develop this content, and, therefore, has no control over it.

- A. **Content Standard for General Internet Content** - The Internet is a free marketplace of ideas. Currently, no industry standards apply to content on the Internet. However, Verizon Online offers content management tools to help customers establish appropriate controls regarding the content that is accessible through their computer, and, in the process, Verizon Online helps parents and other users control the types of content that they and their families can access online. These tools include parental controls offered by Verizon Online and by its portal partners, as well as an Internet Safe Search feature to help control search results initiated from Verizon Online websites.

## Verizon Wireless' General Content Guidelines

### 1. Content Generated By Or On Behalf of Verizon Wireless:

This content category covers content Verizon Wireless generates or produces or that a third party produces or generates on Verizon Wireless' behalf. This content is so closely identified with the Verizon Wireless brand that one could reasonably assume Verizon Wireless has given the content its approval. Examples of content in this category include some of the video clips distributed through V CAST Video (e.g. V CAST Today video clips) and some of the applications distributed through Get It Now (e.g., VZ Navigator, VZW Tones, VZW Pix).

Advertising, user generated and short code-based messaging campaigns used for purposes other than distributing content are not covered by these guidelines. They are addressed below by separate guidelines.

A. Content standard for this category - Verizon Wireless will only distribute content in this category that is lawful and does not otherwise fall into the categories of excluded content described below. Verizon Wireless will not knowingly distribute any content in this category that includes material described below:

- Content that contains anything that is obscene or indecent or anything with strong sexual, explicit or erotic themes or that links to such content; or
- Content that contains hate speech; or
- Content that contains excessive violence; or
- Content that contains extreme profanity; or
- Content that contains misleading or fraudulent claims; or
- Content that promotes or glamorizes alcohol abuse, illegal drug use or use of tobacco products.

Consistent with prevailing standards in other content distribution mediums, content in this category that does not satisfy the above guidelines may be distributed by Verizon Wireless if included in the context of artistic, educational, medical, news, scientific or sports material.

Content in this category must also comply with applicable industry standards (e.g., Mobile Marketing Association's Best Practices, CTIA's Wireless Content Guidelines).

### 2. Third-Party Content Verizon Wireless Distributes On A Verizon Wireless-Branded Distribution Platform:

This content category covers content distributed through Verizon Wireless-branded distribution platforms such as Get It Now, V CAST Mobile TV, V CAST Music, V CAST Video and short code-based messaging campaigns. Some of this content is rated, while other content is unrated. Content management tools are available to limit or restrict access to this content.

This content must be lawful and comply with applicable industry standards (e.g. Mobile Marketing Association's Best Practices, CTIA's Wireless Content Guidelines, etc.). Content distributed through Verizon Wireless-branded distribution platforms cannot disparage Verizon Wireless or its affiliates.

The content standards for content in this category are described below:

- A. **Content Standard for Rated Content - Third-party groups have rated this content and content management tools, such as parental controls and service blocks, are available to limit or restrict access to this content. Verizon Wireless will leverage existing ratings systems and make content management tools available in connection with the distribution of this content. Equipped with these tools, customers are empowered to make their own choices about the types of content they choose to access. Verizon Wireless may, in its discretion, elect not to carry certain types of content based on, among other things, ratings and prevailing industry practices.**
- B. **Content Standard for Content That is Not Rated - Content in this category has not been rated. However, content management tools, such as parental controls and service blocks, are available in connection with the distribution of this content to enable customers to limit or restrict access to the content. Examples of content in this category include unrated wallpaper and ringtones distributed through Verizon Wireless' Get It Now platform.**

Verizon Wireless will encourage its content providers to rate content they seek to distribute over a Verizon Wireless-branded distribution platform. If, however, the content is not rated, Verizon Wireless will not distribute any such content unless it complies with the requirements contained in Category 1 above.

3. **Content To Which Verizon Wireless, As A Network Provider, Provides Access:**  
Content in this category covers content that Verizon Wireless, in its role as a network provider, enables customers to access on the Internet, but which Verizon Wireless does not generate, own or control (e.g. content that a user accesses by browsing or searching). This content includes the vast range of content available on the Internet using mobile devices.

**Content Standard for General Internet Content - The Internet is a free marketplace of ideas. Currently, there are no industry standards that apply to content on the Internet. However, Verizon Wireless offers content management tools to help customers establish appropriate controls regarding the content that is accessible to them from the Internet via their mobile devices. These tools include parental controls and service blocks.**

---

## Verizon Wireless' Short Code Messaging Content Guidelines

Short code-based messaging campaigns vary widely. The following standards apply to the various categories of short code messaging.

- 1) Campaigns used to distribute content (e.g., wallpapers, ringtones, games, videos, jokes, horoscopes, alerts, etc.) to customers of Verizon Wireless must comply with Verizon Wireless' General Content Guidelines.
- 2) Campaigns used to advertise, promote or market companies, goods or services (e.g., coupons, offers, brand awareness, marketing-oriented sweepstakes and contests, etc.) to customers of Verizon Wireless must comply with Verizon's Advertising Content Guidelines.
- 3) Campaigns used to provide services that enable posting or transmission of user-generated content (e.g., chat or flirt programs, communities, bulletin boards, blogs, photo or video portals, social networks, etc.) by customers of Verizon Wireless must comply with Verizon's User Generated Content Guidelines.

All other campaigns, including campaigns of political and advocacy groups, will be governed by the policy set forth in the letter of Lowell C. McAdam, President and Chief Executive Officer of Verizon Wireless, to The Honorable John D. Dingell dated September 28, 2007. Under that policy, Verizon Wireless will provide short code-based messaging services to any group that is delivering legal content to customers who affirmatively indicate that they desire to receive such content.

All short code-based messaging campaigns provided to customers of Verizon Wireless must comply with applicable industry standards (e.g., Mobile Marketing Association's Best Practices, CTIA's Wireless Content Guidelines, etc.).

---

## Verizon Business' Content Guidelines

As a network provider, Verizon Business provides business, government and wholesale customers with access to the Internet and, through it, to services and content which Verizon Business does not own, develop or control.

Verizon Business respects freedom of expression and our customers' ability to freely access and disseminate the lawful content of their choosing in a manner that respects others' use of the network and that complies with the law.

All use of Verizon Business' Internet Services and related equipment and facilities must comply with Verizon Business' Acceptable Use Policy, available online at <http://www.verizonbusiness.com/terms>.

## Verizon's User Generated Content Guidelines

These guidelines apply to services that enable the posting or transmission of content that users generate (e.g., chat or flirt programs, communities, bulletin boards, blogs, photo or video portals, social networks, etc.); in other words, "User Generated Content Services" or "UGC Services." These guidelines apply to UGC Services hosted by others but offered on a Verizon-branded content platform (Section I), and to UGC Services that are hosted by or on behalf of Verizon (Section II).

### 1. User Generated Content Services Provided by A Third Party on a Verizon-Branded Content Platform.

A third party User Generated Content Service appearing on a Verizon-branded content platform must comply with the law and have in place a set of sound practices which incorporate safeguards aimed at protecting users of the services from abuse, fraud and other inappropriate conduct or activities. These safeguards should, in particular, protect children and adolescents from predators and inappropriate content.

Sound practices may evolve over time, but third party UGC Service policies under this category should include, at a minimum, the following:<sup>1</sup>

- Prominent disclosure of the existence and nature of the safeguards on or through the provider's delivery platform (e.g., websites and other applications);
- Assurances that relevant business practices conform to the disclosures made about the safeguards;
- Processes to accept complaints from users of the services about nudity, pornography, harassment, unwelcome contact, fraud or other inappropriate conduct or activity via hyperlinks prominently placed throughout the provider's delivery platforms or other complaint reporting mechanisms; and
- Processes to immediately (within 24 hours) acknowledge receipt of a complaint about inappropriate conduct or activity and promptly (within three business days) provide an explanation to the complainant of the steps taken to address the complaint.

While the above sound practices represent the minimum basic elements that UGC Service providers should include in their practices, such providers can and should have additional requirements that are customized to the unique characteristics of their individual services.

Additionally, third party hosted UGC Services should adopt policies and practices to ensure compliance with the law, including appropriate notice and take-down procedures for unlawful content.

<sup>1</sup> These requirements are consistent with evolving industry standards, such as those adopted by Facebook. See "Facebook Content Code of Conduct," <http://register.facebook.com/codeofconduct.php>, and "Facebook Terms of Service," <http://www.facebook.com/terms.php>.

User Generated Content Services in this category must also comply with applicable industry standards (e.g., Mobile Marketing Association's Best Practices, CTIA's Wireless Content Guidelines, etc.). These guidelines apply to any User Generated Content Services that will be included on Verizon-branded content platforms as well as to short code-based messaging campaigns that will be used to provide such services.

## **2. User Generated Content Services Verizon Hosts Or User Generated Content Services Hosted On Verizon's Behalf.**

UGC Services offered and hosted by Verizon or that are hosted by a third party on Verizon's behalf must comply with the minimum sound practices referenced in Section 1 above.

Hosted UGC Services in this category generally fall into two groups: those that are "open" (e.g., publicly accessible) and those that are "closed" (e.g., not publicly accessible). Verizon supports the use of proactive controls on "open" UGC Services, where they are commercially available, to help identify and protect against user generated content that is offensive or unlawful, or content that fails to comply with the UGC Service's terms of use or acceptable use policy. For "closed" communities or sites, Verizon generally will not provide (or require others to provide) proactive controls.

Verizon will provide an acceptable use policy for its UGC Services that is consistent with Verizon's Guiding Principles for Content, and all users will be required to comply with the policy as a condition of their continued use of Verizon's UGC Services.

In all cases, UGC Services that Verizon offers will comply with the law, including applicable notice and take-down requirements for unlawful content.

User Generated Content Services in this category must also comply with applicable industry standards (e.g., Mobile Marketing Association's Best Practices, CTIA's Wireless Content Guidelines, etc.).

## Verizon's Advertising Content Guidelines

These advertising guidelines apply to third party advertisements, which appear on Verizon-branded websites or platforms and are part of a Verizon-controlled advertising inventory ("Advertisements" or "Advertising"). These guidelines also apply to short-code based messaging campaigns that advertise or promote companies, goods or services (e.g., coupons, offers, brand awareness, marketing-oriented sweepstakes or contests, etc.). These guidelines do not apply to advertising that may appear on a non-Verizon website, or on a Verizon-branded website or platform where Verizon does not control the advertising inventory.

Verizon maintains an advertising review group that examines Advertising for compliance with these guidelines. Wherever practicable, Verizon's advertising review group will review Advertising prior to publication.

Verizon may reject Advertisements which it believes are misleading, inaccurate, or which make fraudulent or unfair competitive claims. Verizon may also reject Advertisements which, in our judgment, make insufficiently supported claims or claims that distort the true meaning or practical application of statements made by the advertiser. Advertisements may not contain material that is patently offensive or which violates the law (e.g., libel, copyright, trademark, right of privacy, etc.). Additionally, Verizon may reject Advertisements which fail to comply with Verizon's standards of decency and good taste.

All Advertisements must comply with applicable industry standards (e.g., Mobile Marketing Association's Best Practices, CTIA's Wireless Content Standards, etc.). All Advertising should also comply with applicable advertising standards adopted by various associations for specific products and services such as the advertising guidelines adopted by the Distilled Spirits Council of the United States and the Children's Advertising Review Unit of the Council of Better Business Bureaus.

Verizon's Advertising Content Guidelines are based on industry practices and do not purport to include an exhaustive list of all types of Advertising Verizon would find objectionable. As part of Verizon's commitment to provide the highest quality services and experience to its customers, Verizon will not accept certain types of Advertising. For example, in addition to the foregoing, Advertisements may not contain any material that Verizon, in its discretion, deems to fall into the following categories or that links to such material:<sup>2</sup>

- Anything that is obscene or indecent or that contains strong sexual, explicit or erotic themes; or

<sup>2</sup> The bulleted restrictions are based on similar restrictions in the publicly available advertising guidelines of Google and The New York Times.

- Products or sites depicting or providing how-to materials about pedophilia or other non-consensual contact; or
- Products or sites that suggest the availability of prostitution services; or
- Products or sites that advocate, glorify or promote rape, torture, cannibalism, suffering or death; or
- Individuals seeking to adopt children or who offer children for adoption; or
- Products that descramble cable or satellite signals in order to get free services; or
- Products that promote software or techniques that bypass copyright protections; or
- Counterfeit, fake or bootleg products or replicas or imitations of designer products; or
- Promotes nudity, nude beaches or naked cruises or resorts; or
- Products or sites that appear to facilitate or promote the evasion of laws (e.g., radar detectors, etc.); or
- Products made from endangered species; or
- Products or sites that offer fake identification or falsified documentation; or
- Promotes the sale of firearms or ammunition by mail order or at gun shows; or
- Products or sites that have online gambling as a central theme; or
- Promotes services, contests or games that predict winners of races or sporting events; or
- Trivializes historic events such as the Holocaust, the Irish Famine or September 11<sup>th</sup>; or
- Hunting trips that guarantee animals will be available for kill; or
- Multilevel marketing schemes; or
- Organ transplant services; or
- Products or sites that guarantee credit repair or credit cards; or
- Products or sites of questionable legality (e.g., miracle cures, etc.); or
- Escort services or "strip" clubs; or
- Hate speech; or
- Excessive violence; or
- Defamatory, libelous or threatening sites; or
- Extreme profanity; or
- Depicts, promotes or is designed to facilitate alcohol abuse, illegal drug use or use of tobacco products.

Verizon reserves the right to reject Advertisements that promote competitors of Verizon and Advertisements that harm Verizon's brand or public image.

If Advertisements contain statements or illustrations that are not deemed acceptable and that Verizon thinks should be changed or eliminated, Verizon may, at its election, notify the advertiser. Verizon may attempt to negotiate changes to the Advertisements with the advertiser, but is not obligated to do so.



For information about industry standards, visit:

CTIA CONSUMER CODE:  
[www.ctia.org/content/index.cfm/AID/10352](http://www.ctia.org/content/index.cfm/AID/10352)

CTIA CONTENT GUIDELINES:  
[www.ctia.org/advocacy/policy\\_topics/topic.cfm/TID/36](http://www.ctia.org/advocacy/policy_topics/topic.cfm/TID/36)

MOBILE MARKETING ASSOCIATION'S BEST PRACTICES:  
[www.mmaglobal.com/bestpractices.pdf](http://www.mmaglobal.com/bestpractices.pdf)

CHILDREN'S ADVERTISING REVIEW UNIT OF THE COUNCIL OF BETTER BUSINESS BUREAUS:  
[www.caru.org/guidelines](http://www.caru.org/guidelines)

To download an informal brochure describing Verizon's Content Policies, visit:  
[verizon.com/contentpolicy](http://verizon.com/contentpolicy)

Verizon Communications Inc. (NYSE: VZ), headquartered in New York, is a leader in delivering broadband and other wireline and wireless communication innovations to mass market, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, serving nearly 66 million customers nationwide. Verizon's Wireline operations include Verizon Business, which delivers innovative and seamless business solutions to customers around the world, and Verizon Telecom, which brings customers the benefits of converged communications, information and entertainment services over the nation's most advanced fiber-optic network.

A Dow 30 company, Verizon employs a diverse workforce of nearly 235,000 and last year generated consolidated operating revenues of \$93.5 billion.

For more information about Verizon, please visit:  
[verizon.com](http://verizon.com)

**Mary Louise Weber**  
Assistant General Counsel



**Verizon Communications Inc.**  
One Verizon Way, Rm VC54S440  
Basking Ridge, New Jersey 07920  
Phone 908-559-5636  
Fax 908-698-2067  
mary.l.weber@verizon.com

November 21, 2008

**By Federal Express**

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

Dear Mr. Kron:

I am writing to acknowledge receipt on November 17, 2008 of the shareholder proposal submitted by Trillium Asset Management Corporation ("Trillium") on behalf of its clients who are beneficial owners of Verizon Communications Inc. common stock (the "Proponents") for inclusion in the proxy statement for the 2009 Verizon Communications Inc. annual meeting of shareholders.

Under the Securities and Exchange Commission's (SEC) proxy rules, in order to be eligible to submit a proposal for the 2009 annual meeting, the proponent must have continuously held at least \$2,000 in market value, or 1%, of Verizon's common stock for at least one year prior to the date that the proponent submits the proposal. In addition, the proponent must continue to hold at least this amount of the stock through the date of the annual meeting. The proposal, including any accompanying supporting statement, may not exceed 500 words. For your reference, I have attached a copy of the SEC's proxy rules relating to shareholder proposals.

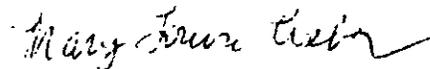
Please provide us with the name(s) of the Proponents whom you represent, together with a written statement from each Proponent authorizing you to act on such Proponent's behalf with respect to the submission of the proposal. In addition, please provide a written statement from the record holder of each Proponent's securities verifying that, at the time the Proponent submitted the proposal, the Proponent had continuously held the requisite number of shares of

Verizon common stock for at least one year. The SEC rules require that this documentation be postmarked or transmitted electronically to us no later than 14 days from the date you receive this letter.

Once we receive this documentation, we will be in a position to determine whether the proposal is eligible for inclusion in the proxy statement for the Verizon 2009 annual meeting.

Please do not hesitate to contact me if you have any questions.

Kind regards,

A handwritten signature in cursive script that reads "Mary Louise Weber".

Mary Louise Weber

Enclosures

cc: Marianne Drost

EXHIBIT "F"

*charles* SCHWAB  
INSTITUTIONAL

PO Box 628290 Orlando Florida 32862-8290

November 26, 2008

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

Re: Richard Ames/Schwab Account

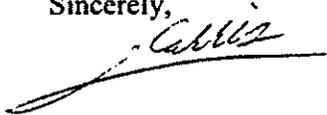
Dear Ms. Weber

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 Verizon Communications, Inc. (VZ) These shares have been held continuously for at least one year prior to and through November 17, 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

END