Before
The Federal Trade Commission
Washington, D.C. 20580

In the Matter of

"Exploring Privacy" Roundtables – Comment
Project No. P095416

COMMENTS OF
OPEN MEDIA AND INFORMATION COMPANIES INITIATIVE
(Open MIC)

Submitted by:

Michael Connor
Executive Director
Open Media and Informational Companies Initiative (Open MIC)
55 West 39th Street
Suite 800
New York, N.Y. 10018
212-537-9401
mconnor@openmic.org

October 16, 2009

COMMENTS OF
OPEN MEDIA AND INFORMATION COMPANIES INITIATIVE

1. BACKGROUND

The Open Media and Information Companies Initiative – or Open MIC (www.openmic.org) – is a non-profit media advocacy organization that works to promote a vibrant, diverse media environment through market-based solutions.

Launched in 2007, Open MIC organizes shareholders of publicly-held media and information technology companies to bring about responsible corporate management policies; our organizing principle is that a dynamic, open and critical media sector is good for both the business of media and the health of democratic society.

Members of the Open MIC coalition are investors, investment advisory and mutual fund companies, foundations and shareholder advocacy groups with a combined total of more than $100 billion in assets under management. Members include leading socially responsible investment firms Boston Common Asset Management, Calvert Asset Management Company, Domini Social Investments, Harrington Investments and Trillium Asset Management Corporation; the As You Sow Foundation; and the New York City Pension Funds.

Privacy is a core issue for Open MIC. To date the organization has focused largely on the practices of U.S. Internet Service Providers (ISPs); a particular concern has been behavioral advertising and the deployment of "deep packet inspection" and content filtering technologies by ISPs.

In late 2008 and early 2009 , the Open MIC coalition wrote letters and introduced shareholder resolutions at publicly-held ISPs seeking reports from their boards regarding Internet network management practices and their impact on Internet privacy and freedom of expression.

Several of ISPs where shareholder resolutions were filed had attracted considerable public scrutiny by entering into business relationships with an online advertising company, NebuAd, which allowed for targeted advertising to customers based on which Web sites the customers liked to visit. Importantly, customers were required to "opt-out" of a program in which many were not aware they were enrolled.

At two of those ISPs - CenturyTel, Inc. and EarthLink, Inc. – investors controlling stock worth almost $1 billion voted in favor of the Open MIC resolutions. At CenturyTel, the resolution received a remarkable 30% of the vote – a clear expression of shareholder concern. A third ISP, Knology Inc., agreed to revise its Internet privacy policy following the filing of a shareholder resolution.

As investors with a long-term view of value creation, members of the Open MIC coalition believe the Internet offers enormous opportunities for our economy and society. The potential of the Internet to open new markets for commerce, new venues for cultural expression and new modalities of civic engagement is without historic parallel.

We believe it is critical to the financial strength of these companies that Internet advertising grow in both volume and profitability. We have also concluded that Internet commerce is a critical economic driver; as widely diversified investors, we consider broad-based

economic growth important to increasing the value of our portfolios. Accordingly, we view threats to the health of Internet-based commerce as a material issue.

To ensure the growth of this digital economy, Internet users and consumers must trust the online marketplace and its handling of their personal data. That is why Open MIC has sought to persuade the ISPs' managements that providing greater *transparency* and *accountability* for their network management practices is in the corporations' and their shareholders' best interests.

We believe that failure to provide greater transparency regarding privacy practices will weaken consumers' confidence in the firms and their willingness to protect consumers' privacy and freedom of expression. Such failure will also heighten the companies' perceived risk and penalize their share values.

Regulation vs. Self-Regulation

In inviting comment on the issue of privacy, the Commission asks: "Do the existing legal requirements and self-regulatory regimes in the United States today adequately protect consumer privacy interests?"

The network management practices of ISPs have the potential to threaten the privacy of millions of Americans and should command the attention of corporate management, legislators and regulators. As noted by privacy expert Paul Ohm of the University of Colorado Law School:

> Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP). ISPs carry their users' conversations, secrets, relationships, acts, and omissions. Until the very recent past, they had left most of these alone because they had lacked tools to spy invasively, but with recent advances in eavesdropping technology, they can now spy on people in unprecedented ways. Meanwhile, advertisers and copyright owners have been tempting them to put their users' secrets up for sale, and judging from a recent flurry of

> reports, ISPs are giving into the temptation and experimenting with new forms of spying. This is only the leading edge of a coming storm of unprecedented and invasive ISP surveillance.[1]

Some of the greatest threats in this context arise from Deep Packet Inspection technologies, and related content filtering applications, which have the potential to severely inhibit an open and free Internet; they can be misused or otherwise subject consumers – and companies - to new risks.

A recent example highlighting these concerns is the recent deployment of content filtering outside the U.S. by governments in Iran and China to suppress political and social dissent and curb a free and open Internet.

In the U.S., there are numerous pressures on ISPs to use filtering technologies for commercial purposes. For example, copyright owners such as NBC Universal have asked the Federal Communications Commission (FCC) to require that ISPs "use readily available means to prevent the use of their broadband networks to transfer pirated content," an opinion shared by others, such as the Recording Industry Association of America.

However, to make that determination, ISPs must rely on software that is inherently flawed. As a result, copyright filters are considered to be over-inclusive when blocking content and have the potential to interfere with, and suppress, legal expression.

[1] Paul Ohm, "The Rise and Fall of Invasive ISP Surveillance," University of Colorado Law School, August 2008. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344

Filtering Internet content is a significant public policy issue; failure to publicly address this issue poses potential competitive, legal and reputational harm to ISPs. Legal liabilities are posed by FCC regulations, the Wiretapping Act and unfair business practice laws.

Content filtering could also undermine the so-called "safe harbor" provisions under the Digital Millennium Copyright Act and risk violating the Electronic Communications Privacy Act. The Internet Freedom Preservation Act of 2009 now before Congress could present new challenges and demonstrates increasing public concern.

Operating successfully in this terrain requires a strong and public strategic vision from the corporate leadership of ISPs, which need a set of guiding management principles that will allow them to prosper financially and responsibly address their social impact.

However, when asked by shareholders to review and report on these issues – as requested in shareholder resolutions filed by members of the Open MIC investor coalition – several major ISPs went to considerable effort to avoid consideration of the issues.

As the result of management opposition, the Open MIC resolution was not placed on shareholder ballots at Comcast, AT&T, Verizon, SprintNextel and Qwest. In its brief to the Securities and Exchange Commission opposing the Open MIC resolution, for example, AT&T argued that the protection of customer privacy is a management function not subject to stockholder oversight. Stunningly, the SEC staff agreed.

What is most troublesome about the position espoused by AT&T (and other ISPs) is that it focuses extremely narrowly on the language of privacy policies that are difficult to fathom and pertain only to AT&T's subscribers. The reality is that ISP Internet network management practices affect many more people than the customers of any one company, owing to the

practice of “peering” in which multiple networks are used by a vast array of Internet users as their data and content are transmitted across the Internet. In that way, the potential harms of Deep Packet Inspection and filtering technologies threaten a population of people far broader than a single company’s customers.

As long as Internet network management practices are developed in secret, Americans can expect that their worst fears may be realized, with persistent challenges to their freedom of expression and privacy. ISPs are managing and discussing Internet networks in a manner that provides the public with little or no meaningful understanding of how their privacy and freedom of speech interests are protected. The risks associated with this approach are untenable. It is time for companies to stop hiding behind the legal jargon in their privacy policies and “terms of use” and, instead, address these issues directly.

Unfortunately, we’ve concluded, at least for the moment, that the media and marketing industries have largely failed to develop and promote adequate safeguards for consumer privacy. It is clear that allowing the industry largely to police itself and determine its own risk levels is unacceptable. Such a course raises concern regarding the value of individual companies as well as a broader risk to the entire economy, something long-term highly diversified investors find particularly concerning.

2. **Protecting Privacy – Human Dignity – Economic Growth**

There is abundant evidence that the American public is concerned about privacy. A recent study by researchers at the University of Pennsylvania and the University of California, Berkeley, found that “contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are

informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages— between 73% and 86%--say they would not want such advertising."[2]

Feeding this concern, we believe, is the basic notion that privacy is a fundamental human right – not something that should be bargained away easily in exchange for ease-of-use in Internet shopping. In this context, consumers perceive violations of individual privacy as violations of basic human dignity.

Article 12 of the Universal Declaration of Human Rights states, for example, that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) holds that "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

As investors, we believe the commercial opportunities afforded by the Internet – and these concomitant obligations to respect privacy and human dignity – can only be addressed through a long-term corporate management strategy. Indeed, consumers and investors continue to grapple with the effects of the recent (and ongoing) global economic crisis, fed in no small measure by the finance industry's undue emphasis on short-term return-on-investment.

[2] Joseph Turow et al., "Americans Reject Tailored Advertising," University of Pennsylvania and University of California, Berkeley, September 2009. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214

We see these issues – privacy protections and economic growth – as inexorably linked. The University of Pennsylvania/UC Berkeley survey data suggest that there is deep distrust and questioning of online practices. If those concerns are exacerbated and lead to people discontinuing online economic activity, we believe the direct and indirect impacts could be substantial for our portfolio companies.

3. Failure of Industry Recommendations

While we realize that technology changes quickly, and that regulation of technology is particularly challenging, as investors we are convinced that the long-term interests of business and society will be best served by the development of sound policies and practices that are easily understood and implemented.

We have carefully considered two recent analyses and sets of proposals regarding behavioral targeting and behavioral advertising. The first, published in July 2009, is a set of "self-regulatory principles" put forth by a coalition of advertising industry associations[3]; the second is a set of concerns and "proposed solutions," published in September 2009 and put forth by a coalition of consumer and privacy advocacy organizations. [4]

As socially responsible investors, we would prefer industry self-regulation – indeed, corporate responsibility and corporate engagement with responsible business practices are

[3]Association of American Advertising Agencies, Association of National Advertisers, Better Business Bureau, Direct Marketing Association, Interactive Advertising Bureau "Self Regulatory Principles for Online Behavioral Advertising," July 2009.

[4]Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S, Public Interest Research Group, The World Privacy Forum, "Online Behavioral Tracking and Targeting Concerns and Solutions," September 2009

critical elements of the mission for our organizations. In that context, we welcome the industry's proposed self-regulatory scheme. Particularly appealing, from our perspective, is a proposed principle related to "Education" and a proposed commitment to more fully explain online behavioral advertising to consumers and businesses.

However, we note that the industry proposals lack detail and fall far short of presenting the innovative approaches to privacy protection that we would expect of corporate management with a long-term perspective toward shareholder value creation. As but one example, this is the entirety of the industry's proposed principle on "Sensitive Data" as it pertains to Financial and Health data:

> Entities should not collect and use financial account numbers, Social Security numbers, pharmaceutical prescriptions, or medical records about a specific individual for Online Behavioral Advertising without Consent.[5]

Among other weaknesses, this proposed principle leaves vast openings for marketers and advertisers to build behavioral profiles of consumers based, for example, on their Internet searches for information regarding financial subjects such as unemployment or bankruptcy; personal subjects such as divorce or sexual identity; and medical subjects specific to a particular disease or ailment. One can imagine, without much difficulty, how such information might be used to unfairly discriminate against people in a way that would affect an individual's credit, education, employment, insurance or access to government benefits.

Indeed, in its expanded "Comments" on its own principles, the industry says, with regard to Financial and Health data:

[5] Association of American Advertising Agencies et al., op. cit., p. 17

> This is a complex area and there may need to be additional areas that should fall into the sensitive data category. The entities participating in the development of these Principles intend to evaluate such areas if and when they may arise in the marketplace.[6]

In other words, if forced to consider these issues more directly, the industry will. What is especially troublesome to us, as investors, is that these proposed principles for self-regulation were arrived at and published after considerable debate, analysis and reflection within the advertising and marketing communities. Surely the industry associations encountered no shortage of well-paid consultants, experts and lawyers well-versed in the workings of privacy law and regulation; the industry decision to propose a Sensitive Data principle so narrowly focused, and so potentially open to abuse, represents a complete misreading of the American public's sensitivities toward the issue of privacy, as indicated by the recent University of Pennsylvania/UC Berkeley research.

As investors, we find little evidence of innovative or enlightened management on these critical issues of privacy. We find ourselves reluctantly concluding that the best long-term approach to value creation for shareholders requires regulatory or legislative action.

Accordingly, we believe that any new regulation of online advertising should address the following principles:

- Federal privacy law should be based on "opt-in" principles, requiring an affirmation by an individual permitting the collection of personal data and tracking information;
- Users should be allowed to access and erase their digital data, and files about them, as compiled by online marketers and advertisers;

[6] Association of American Advertising Agencies et al., op. cit., p. 40

- Publishers and distributors of Internet browsers should be required to provide technology that permits users to browse the Internet without leaving data trails;
- Particular care and attention should be given to respecting personal dignity and to protecting consumer information, including individual medical and financial data, that could be used for purposes other than those intended by the Internet user.
- Consumers should be provided with strong and transparent consumer protections related to the secondary uses of personal information. So-called information accountability regimes modeled on consumer lending laws offer a promising template for such protections.
- Data should be retained for no more than 24 hours without obtaining an individual's consent.

As responsible investors, we believe in maximizing revenue and profitability while also respecting the privacy rights of individuals. In fact, we are convinced that the best way to encourage long-term growth of the Internet is to encourage responsible management practices that foster transparency, accountability and trust.

We thank the Commission for the opportunity to comment on this pressing social policy issue and stand ready to discuss our positions further with the Commission or members of its staff.