



The Open MIC Internet Project: A Shareholder Initiative

"The Internet has been the most fundamental change during my lifetime and for hundreds of years."

Rupert Murdoch, CEO, News Corp.

"If consumers feel that Internet companies are not protecting their privacy, the Internet's ability to serve as an engine of economic growth will be threatened."

Michael Hintze, Associate General Counsel, Microsoft,
testifying before Congress on Internet privacy

"The dirty little secret of the Internet industry is that all the providers use software tools to manage their network traffic. Comcast got caught and may have been more aggressive than some rivals, but it's certainly not alone."

Vindu Goel, reporting on the FCC's ruling against Comcast
in the *New York Times*

"These technologies—filtering, monitoring, deep packet inspection—are exactly the same technologies that are the technology of censorship. AT&T and Comcast want to use them for commercial advantage...I am suggesting that it is a small step from censorship for commercial advantage to censorship for other reasons."

Professor Tim Wu, Columbia University School of Law
testifying before Congress on Internet censorship

"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..."

Jeffrey Rosen
George Washington University School of Law
New York Times Sunday Magazine 11/28/2008

Executive Summary: Privacy, Free Speech and the Future of the Internet

The Internet is transforming life in the 21st century. The digital revolution has created unprecedented opportunities for economic, cultural and democratic participation in society. We need look no further than to Google in the commercial arena, YouTube in the cultural or Barack Obama in the political to see such opportunity at work. Unknown a decade ago, each has used the Internet to revolutionize their respective fields of endeavor.

These opportunities arose in a U.S. Internet environment where freedom of expression and the right to privacy have been respected in large part. This respect has encouraged participation, expression, competition and innovation. These rights, however, are neither inherent nor necessary to the technology of the Internet. This same technology poses dire threats to our privacy and freedom of expression and thereby to the competitive vigor of free markets. China's iron-fisted control of its domestic Internet offers chilling testament to this fact.¹

Such threats are not posed solely by foreign governments to foreign consumers, however. There is now sufficient evidence of corporate infringement of US consumers' rights to privacy and freedom of expression on the Internet. While the companies' motives may be commercial rather than political, the threats are no less real. They jeopardize not only our privacy and most cherished political freedom, but the openness and inclusiveness that have made the Internet an engine of opportunity and innovation.

The Open MIC Internet Project is a growing coalition of progressive investors dedicated to preserving and promoting the openness of the Internet environment. Members include Trillium Asset Management Corp., Boston Common Asset Management, Calvert Asset Management Company, Domini Social Investments, Harrington Investments, the As You Sow Foundation and The New York City Pension Funds. The NYC Pension Funds have over \$100 billion in assets and are among the top 20 shareholders of most major Internet Service Providers (ISPs).

Members of the coalition press the case with ISPs that respect for consumers' privacy and freedom of expression is not only a political desideratum but a commercial one. As a first step, members of the Open MIC Internet Project have filed shareholder resolutions with 11 ISPs this fall, with additional filings likely. The resolutions urge the companies' Boards to report to shareholders on their network management practices' impact on public expectations of privacy and freedom of expression.

**Copy of Shareholder resolution filed by Trillium Asset Management with AT&T
(Similar resolutions have been filed with other Internet Service Providers)**

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

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

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

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

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

Whereas:

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

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

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

**Open MIC Internet Project
Shareholder Resolutions filed as of 12/10/2008**

AT&T (NYSE:T)
Charter Communications (NASDAQ:CHTR)
CenturyTel, Inc. (NYSE: CTL)
Comcast Corporation (NASDAQ:CMCSA)
EarthLink Inc. (NASDAQ:ELNK)
Embarq Corporation (NYSE:EQ)
Knology Inc. (NASDAQ:KNOL)
Sprint Nextel Corporation (NYSE:S)
Qwest Communications International (NYSE:Q)
Verizon Communications (NYSE:VZ).

Background Data

A Shifting Regulatory Landscape

Most of the firms in question traditionally have been considered “telephone” or “cable” companies. Now, in their function as Internet Service Providers (ISPs), their fixed wireline and wireless broadband offerings are considered “information services” by the Federal Communications Commission--a new regulatory category created in 2005.

Information services are exempt from the “common carriage” regulations that require traditional telecoms to be neutral handlers of transmissions over their lines. This grants ISPs tremendous powers of discretion over the information flows that pass through their networks, both wired and wireless. In this regard they function more like media firms than telecoms.

These ISPs provide and control access to the Internet for tens of millions of Americans. The group includes Verizon Communications Inc., Verizon Wireless (a 50-50 joint venture between Verizon and Vodafone Plc), AT&T Inc., Sprint Nextel Corp., Comcast Corp., Time Warner Inc., Qwest Communications, Charter Communications Inc. and Cablevision Inc. Research in Motion Ltd., creator of the Blackberry handheld device, might also be included in this group by virtue of its own private network which provides email and messaging services to millions of users.

Internet Filtering

These firms in their role as ISPs manage the information flows across their networks through a variety of means. Our concern focuses on the ISPs’ practice of *Internet filtering* – by which we mean any practice whereby consumers are prevented or hindered from accessing or publishing certain information on the Internet.²

While foreign governments’ use (e.g. China) of Internet filtering has been highly publicized, ISPs in the US are using these same techniques as part of their network management regimes. While there may be legitimate uses of such techniques, there is documented evidence of *illegitimate* use that constitutes unjustified censorship and invasion of privacy (see Appendix A).

A review of the case evidence does not suggest a single theme or motivating interest behind the practice. Rather, as detailed below, incidents appear to have been prompted by various factors arising in many different service settings.

The disturbing conclusion is that these incidents appear to reflect rather arbitrary management practices employed on an *ad hoc* basis. Across the board, ISPs’ managements are tight-lipped

about what, if any, policies they've developed to govern their use of Internet filtering techniques. If there are such policies, they have been developed and continue to be held in secret.

The Open MIC Internet Project is aimed squarely at this unacceptable reticence. For ISPs to vouchsafe their Internet filtering as "legitimate" without disclosing their criteria for making such judgments is a meaningless gesture. It says nothing more than "trust us." Consumers have a right to know not only *that* but *how* an ISP will protect their privacy and respect their freedom of expression. Trust, but verify.

For the ISPs, the challenge then is to provide adequate disclosure on these matters while protecting their own legitimate economic interests. To date, they've failed at that task, as evidenced by multiple embarrassing incidents played out in the court of consumer opinion.

These incidents have prompted proposed legislation in the House and Senate; a formal Federal Communications Commission investigation of network management practices; civil lawsuits; and numerous high-profile complaints by civic and media policy groups.

As the growth of digital media accelerates – with new electronic devices, new forms of delivery, and increased demand for Internet bandwidth – Internet filtering, consumer privacy and freedom of expression will increasingly be front-page issues, commanding shareholder attention.

A Shareholder Response

The Open MIC Internet Project has brought together a coalition of investors to engage the publicly held ISPs that manage the wired and wireless networks that constitute the Internet.

The coalition will seek to impress upon the ISPs' managements that providing greater transparency and accountability for their network management practices is in the corporations' and their shareholders' best interests.

The coalition will argue that failure to provide greater transparency about these practices will weaken consumers' confidence in both the firm and its willingness to protect consumers' privacy and freedom of expression. In a competitive environment where brand value and consumer trust are often decisive factors in consumer choice, such transparency will prove a competitive advantage. Failure to provide such transparency will prove a competitive disadvantage.

The coalition will also argue that failure to provide greater transparency about these practices will limit investors' ability to assess brand risk as well as the risk of legislative or regulatory intervention to protect consumers' rights. In an investment climate where ESG³ risks are increasingly included in share-valuation analyses, such failure will heighten a firm's perceived risk and penalize its share values.

Corollary to this needed transparency are management structures that create and insure accountability for a firm's network management practices.

Similar to the Carbon Disclosure Project and the Center for Political Accountability's donation reporting, these disclosures are an important first step to insuring that the Internet remains an engine of increasing opportunity, innovation, inclusion and expression.

We expect to file shareholder resolutions with several of the ISPs. The resolutions will be filed in the fourth quarter of 2008 in time for consideration during the spring 2009 proxy season.

1. China's domestic internet is discussed at length in *Who Controls the Internet?: Illusions of a Borderless World*, by Tim Wu and Jack Goldsmith, Oxford University Press, 2006.

2. We borrow the term 'internet filtering' here from John Palfrey's paper, "Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet" from *GLOBAL INFORMATION TECHNOLOGY REPORT, World Economic Forum, 2006-2007*

Appendix A: Case Examples of Corporate Internet Filtering in the US.

In each of the following cases a company with control over large portions of our communications infrastructure restricted the freedom of expression of its customers and/or invaded their privacy. In each case the company had no reason to believe the customers involved were breaking any law or regulation. Americans have a right to know why these companies did what they did--and how they will handle similar situations in the future.

1. Comcast actively interferes with Internet use.

In August 2008 the Federal Communications Commission voted to punish Comcast Corp., the nation's largest cable company, for violating agency principles that guarantee customers open access to the Internet.

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.

After initially denying that it interfered with customer service, Comcast acknowledged that it had used "reset" packets to "delay" some peer-to-peer traffic as part of a "reasonable network management" practice.

In announcing the FCC's ruling, commission Chairman Kevin Martin said Comcast's network management amounted to "looking inside its subscribers' communications, blocking that communication when it uses a particular application regardless of whether there is congestion on the network, hiding what it is doing by making consumers think the problem is their own, and lying about it to the public..."

Three class-action lawsuits have been filed against Comcast in California, Illinois, and New Jersey, alleging that the company deceived and misled consumers by advertising that it offered "unfettered access to all the content, services, and applications that the Internet has to offer."

Comcast argues that the FCC's policy statement is not enforceable and that the commission has "never before provided any guidance on what it means by 'reasonable network management.'"

Five major ISPs – Verizon, Time Warner, Sprint, AT&T and AOL - take arbitrary action that limits free speech for those distributing and discussing perfectly legal content on the Internet.

This case involves something that is universally abhorred – child pornography. In June 2008, New York State Attorney General Andrew Cuomo asked major ISPs to clean up their servers and block access to Usenet groups that are spreading child pornography. California's Governor and Attorney General subsequently made a similar request to ISPs in that state.

Usenet is the pre-Web home to some 100,000 discussion groups, only a small fraction of which contain pornography. Indeed, the N.Y. Attorney General's office said it found child pornography on only 88 of the 100,000-plus Usenet groups. Yet five ISPs – Verizon, Time Warner, Sprint, AT&T and AOL – indicated that to varying degrees they had stopped, or would stop, offering customers access to tens of thousands of Usenet discussion areas. In Verizon's case, for example, that included the alt* groups that have been home to free-flowing discussions for over two decades.

According to CNet: "What this means in practice is that, thanks to the New York state attorney general, Verizon customers will lose out on innocent discussions. Verizon is retaining only eight newsgroup hierarchies, even though over 1,000 hierarchies exist. That means not carrying perfectly innocuous – and, in fact, very useful newsgroups like [symantec.customerservice.general](#), [us.military](#), [microsoft.public.excel](#) and [fr.soc.ecomie](#)."

Even some involved with the issue of child pornography have expressed concern about over-reaching by the ISPs. Larry Magid, a member of the board of directors of the National Center for Missing & Exploited Children, wrote that he was troubled by the "free speech" aspects of the ISP actions because "the vast majority of the material in the Alt hierarchy has nothing to do with child pornography."

3. *AT&T proposes Internet filtering to stop copyright piracy*

At the Consumer Electronics Show in January 2008, AT&T senior vice president James Cicconi said the company was exploring methods of Internet filtering to help content providers combat piracy of their materials. As the New York Times noted, the proposal would mean that AT&T would be "sniffing your digital packets, looking for material that violates someone's copyright."

Said AT&T's Cicconi: "What we are already doing to address piracy hasn't been working. There's no secret there...The volume of peer-to-peer traffic online, dominated by copyrighted materials, is overwhelming. That clearly should not be an acceptable, continuing status."

Other members of the panel, including a representative from Microsoft, disagreed with AT&T's position. Other ISPs, including Verizon, have subsequently disagreed as well.

An analysis of AT&T's proposal by Columbia Law Professor Tim Wu:

"The most serious problems for AT&T may be legal. Since the beginnings of the phone system, carriers have always wanted to avoid liability for what happens on their lines, be it a bank robbery or someone's divorce. Hence the grand bargain of common carriage: The Bell company carried all conversations equally, and in exchange bore no liability for what people used the phone for. Fair deal.

AT&T's new strategy reverses that position and exposes it to so much potential liability that adopting it would arguably violate AT&T's fiduciary duty to its shareholders. Today, in its daily Internet operations, AT&T is shielded by a federal law that provides a powerful immunity to copyright infringement. The Bells know the law well: They wrote and pushed it through Congress in 1998, collectively spending six years and millions of dollars in lobbying fees to make sure there would be no liability for "Transitory Digital Network Communications"—content AT&T carries over the Internet. And that's why the recording industry sued Napster and Grokster, not AT&T or Verizon, when the great music wars began in the early 2000s.

Here's the kicker: To maintain that immunity, AT&T must transmit data "without selection of the material by the service provider" and "without modification of its content." Once AT&T gets in the business of picking and choosing what content travels over its network, while the law is not entirely clear, it runs a serious risk of losing its all-important immunity. An Internet provider voluntarily giving up copyright immunity is like an astronaut on the moon taking off his space suit. As the world's largest gatekeeper, AT&T would immediately become the world's largest target for copyright infringement lawsuits."

4. Charter Communications proposes snooping on internet traffic to harvest private data

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.

If a Charter subscriber did not wish to be included, they would be required to fill in a form and actively opt-out of the service; a special "cookie" would be placed on their hard drive to prevent them from receiving ads. However, if a customer switched to a new browser or a new computer, or cleared their hard drive of "cookies," they would once again receive the service.

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

Charter subsequently announced a suspension of its DPI program. But similar initiatives are likely, from Charter and others. The Wall Street Journal noted: "Because cable operators often provide customers with both Internet and TV service, the potential to use intelligence about customers across different platforms -- by, for example, targeting television ads based on Web-

surfing behavior -- has enormous potential, analysts say. But it also sets off some alarm bells. 'It requires crossing a whole series of Rubicons regarding customer privacy,' says Craig Moffett, an analyst at Sanford C. Bernstein. ... Given the importance of the new revenue stream to cable operators, Charter's cold feet are likely to send operators looking for some new approaches -- but not back off entirely. 'They are going to do this, so it's a matter of when and not if,' said Moffet."

5. *AT&T admits to censoring politically-oriented lyrics of a concert on the Internet*

In August 2007, AT&T censored its webcast of a performance by the rock band Pearl Jam, blocking the audio feed when singer Eddie Vedder ad-libbed some non-obscene but politically pointed lyrics. When confronted, AT&T blamed an overzealous sub-contractor but admitted to a "handful" of similar incidents of censorship.

Open MIC and Trillium engaged AT&T management in dialogue on this issue in late 2007 and early 2008. The company disclosed that subsequent to the Pearl Jam episode it had adopted a "new policy" regarding censorship, but that policy apparently applies only to similar web performances. AT&T would not say how the First Amendment is being treated in other service offerings.

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

However, AT&T would not provide Trillium with a copy of its policies.

6. *Verizon Wireless denies access to its wireless network because a subject is too "controversial."*

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