Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	WC Docket No. 07-52
Broadband Industry Practices	)	

DATA FOUNDRY'S COMMENTS

Data Foundry, Inc. ("Data Foundry") respectfully submits these comments in response to the Commission's Notice of Inquiry ("NOI") released April 16, 2007 (FCC 07-31).

A. Statement of Interest.

Data Foundry was established in 1994 and has its headquarters in Austin, Texas. We are a global provider of managed services, and provide Disaster Recovery, Data Center Outsourcing, Managed Data Center, and Business Continuity Work-Site Recovery Services through regionally-dispersed, secure Data Center and Work-Site Recovery facilities that provide 24x7x365 support from state-of-the-art Network Operation Centers. Data Foundry maintains and monitors a scalable, redundant and highly available network infrastructure. Over 1,000 corporate, governmental and quasi-governmental customers across multiple business verticals use our solutions.

Data Foundry does not provide broadband transmission services. Data Foundry buys high capacity transport as a customer, and pays a premium for it. Data Foundry's business in very large part assumes and depends on the ability of broadband customers to fully enjoy and use the IP-enabled devices, applications and services they obtain and choose to employ. Data Foundry's customers reach Data Foundry over high capacity IP connections, often through the Internet. Many of our customers buy high capacity IP connections for the sole or primary purpose of accessing information they store on

servers co-located at a Data Foundry Data Center. They often employ devices, applications and services that operate in the upper layers of the protocol stack (DNS, TFTP, TLS/SSL, FTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, TELNET, ECHO, BitTorrent, RTP, PNRP, rlogin, ENRP, HTTP, *etc.*). Almost every one has business or legal reasons to maintain control over disclosure of their information to third parties.

Data Foundry is not a "content provider" but would be very much impacted if broadband Internet service providers impose service "tiers," practice what has been called "bit discrimination" or take other actions that operate to significantly limit the ability of Data Foundry's customers to reach Data Foundry to upload, download, interact with or change information that is stored on their behalf by Data Foundry. Similarly, persons that are authorized to access the information stored by Data Foundry on behalf of others would suffer from degraded or limited access if broadband Internet service providers impose tiered service. If a telephone company or cable company could prohibit IP based services like FTP or Telnet, or if packets transmitted using disfavored applications or services were degraded, impeded, blocked or put at the end of the line, then customers could not store their essential information using Data Foundry. Presumably, they would be required to use a competing offering that is sold or approved by the broadband provider, or simply do without.

Data Foundry's customers and their patrons have traditional privileges, contractual nondisclosure agreements and statutory obligations to maintain confidentiality of corporate, governmental and individual consumer/citizen proprietary information. They have confidential/trade secret information, which is ***their property***.

They use broadband to transmit confidential information on a regular basis and previously had no concern whether their underlying transmission provider would somehow destroy this confidentiality by inspecting and appropriating the content or reserving the right to do so. The privacy and security of their information is at risk under the current regime and even more at risk in the near future. The Commission must expressly recognize broadband customers "entitlement" to maintain control over and the confidentiality of their own information.

B. Scope of Comments.

Data Foundry is interested in many of the topics identified by the Commission in the NOI. We have chosen, however, to focus on only two specific concerns in our initial comments because they are not likely to otherwise receive the attention they deserve. These comments are responsive to the request in NOI ¶¶ 8 and 11 for (1) information related to "participants'" behavior and practices and whether they are acting consistent with the "Policy Statement"[1] and (2) whether additional "entitlements" should be recognized.

Data Foundry will demonstrate that – contrary to the popular urban myth spread by the dominant providers – almost every broadband Internet provider currently violates the "entitlements" in the Policy Statement in several demonstrable ways. Data Foundry will also explain that providers are or will soon be engaging in practices that violate

[1] Policy Statement, *In the Matters of Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review -- Review of Computer III and ONA Safeguards and Requirements; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, CC Docket Nos. 02-33, 01-337, 95-20, 98-10, GN Docket No. 00-185, CS Docket No. 02-52, FCC 05-151, 20 FCC Rcd 14986, (rel. Sept. 2005).

customer privacy and threaten the security and confidentiality of proprietary, privileged and/or trade secret information held by every company or person that communicates with others using broadband. Customer Choice and Customer Privacy and Security are at risk, notwithstanding the lofty but ultimately empty words in the Policy Statement.

The Commission should expressly recognize that customers are "entitled" to not be "disentitled" and lose dominion over their own property – confidential, proprietary, trade secret and privileged information that the broadband providers intend to appropriate when the information is transmitted over their networks.

C. Erasing the "Entitlements."

When the Commission decided to abandon common carrier treatment of transmission used to support broadband Internet, it was obvious deregulation would leave providers free to engage in practices that are contrary to the public interest. So the Commission proclaimed a "Policy Statement" purporting to maintain "principles" that bear some similarity to a small part of the common carrier rules the Commission was eliminating the same day:

> … the Commission has jurisdiction necessary to ensure that providers of telecommunications for Internet access or Internet Protocol-enabled (IP-enabled) services are operated in a neutral manner. Moreover, to ensure that broadband networks are widely deployed, open, affordable, and accessible to all consumers, the Commission adopts the following principles:
>
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to access the lawful Internet content of their choice.
>
> - *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to connect their choice of legal devices that do not harm the network.

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to competition among network providers, application and service providers, and content providers.

The Commission recognized its "duty to preserve and promote the vibrant and open character of the Internet as the telecommunications marketplace enters the broadband age."[2] Let's be frank around here for a change. The Policy Statement is inadequate and toothless and has done little by way of preserving or promoting the open Internet. To the contrary, its primary function has been an excuse to approve mergers and a shield by broadband providers to stave off legislation. Some mergers have "voluntary" commitments, but Data Foundry has doubts about their enforceability in terms of sanctions or forfeitures. The finding in the Time Warner/Adelphia merger there was "no evidence that the applicants were operating in a manner inconsistent with the Policy Statement"[3] may be technically correct in terms of the record in that case, but as shown below Time Warner does in fact violate the principles in the Policy Statement. It is not alone. None of the providers honor the principles and they do not fear punishment for violations of them.

---

[2] *Id*, ¶ 5.

[3] Memorandum Opinion and Order, *Applications for Consent to the Assignment and/or Transfer of Control of Licenses, Adelphia Communications Corporation (and subsidiaries, debtors-in-possession), Assignors, to Time Warner Cable Inc. (subsidiaries), Assignees; Adelphia Communications Corporation (and subsidiaries, debtors-in-possession), Assignors and Transferors, to Comcast Corporation (subsidiaries), Assignees and Transferees; Comcast Corporation, Transferor, to Time Warner Inc., Transferee; Time Warner Inc., Transferor, to Comcast Corporation, Transferee*, MB Docket No. 05-192, 21 FCC Rcd 8203, 8296-99, ¶¶ 217-23 (2006).

It is often said there are no examples of any violations. This is just not true. One need look no farther than the broadband providers' current, published Terms of Service and Acceptable Use Policies ("TOS/AUP"). Most providers' TOS/AUP contain terms that *prima facie* violate each "entitlement." Attachment A to these comments provides citation and discussion, but a summary of violations, organized by "entitlement" are:

Policy Statement "Entitlement" 1:

- [C]onsumers are entitled to access the lawful Internet content of their choice.

Attachment A shows that every broadband provider's TOS/AUP reserve the right to monitor content and block any content the provider finds to be "objectionable for any reason." The providers also reserve the right to suspend or cancel service if the customer sends or receives "objectionable" content. The providers arrogate to themselves the right to ban far more than "unlawful" content, and they delegate to themselves the sole, unreviewable right to determine what is and is not "objectionable."

Policy Statement "Entitlements" 2 and 4:

- [C]onsumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
- [C]onsumers are entitled to competition among network providers, application and service providers, and content providers.

The second and third "entitlements" are related, in that they purport to protect competition in applications and services, and then consumers' rights to freely run and use applications and services they obtain from entities other than the broadband provider and/or affiliates or others that contract with them. Attachment A shows that broadband providers' TOS/AUP conflict with these two "entitlements" in several ways.

Many broadband provider TOS/AUP prohibit applications that support VoIP, peer-to-peer communications, software-based servers, access to private networks (such as government or corporate networks used for telecommuting) and other applications like Citrix Online, LLC's GoToMyPC® service. GoToMyPC® software installed on a user's computer, for example, is contrary to many TOS/AUP because it (1) could be called a "server"; (2) allows a user on the Internet at a distant location to remotely operate the home computer, which necessarily extends "network content…outside your Premises LAN"; and (3) allows remote file use and transfer, which is a form of "file sharing." Comcast's terms directly outlaw telecommuting, since they preclude users from using the service in a way that results in the user's computer acting "as an end-point on a non-Comcast local area network or wide area network." These Providers cannot in good faith claim they allow consumers "to run applications and use services of their choice." Large parts of these TOS/AUP are dedicated to limiting customer choice with regard to applications and services.

Policy Statement "Entitlement" 3:

- [C]onsumers are entitled to connect their choice of legal devices that do not harm the network.

Attachment A shows that providers also regulate the devices consumers can use in association with broadband service. Wi-Fi is banned or contractually required to be "password protected." A user cannot allow any person not in the family to use a Wi-Fi enabled device as a means to access the Internet, whether on or off the premise. Some providers ban Network Address Translation devices, which means many common off-the-shelf routers are prohibited. These are "legal" devices and they do not harm the network, but their use is controlled, restricted or prohibited in current TOS/AUP.

The Providers may claim they do not actually enforce these terms. That is not true, but is beside the point. Users are contractually prohibited from enjoying their FCC-bestowed Title I "entitlements." The Providers may assert that "file sharing" must be prohibited because it is principally used to violate intellectual property rights. That may or may not be true, but is also beside the point. The TOS/AUP do not distinguish between "infringing" file-sharing and totally lawful "non-infringing" file sharing. The providers will likely defend the ban on Wi-Fi hot spots for any number of reasons, but these devices are widely available for purchase, and there is no national law requiring password protection. The restriction on full use of the Wi-Fi capability according to the purchaser's choice is unquestionably contrary to the plain meaning of the words in the third "entitlement."

The summary above and further description in Attachment A detail current contract terms that directly conflict with the "entitlements" set out in the Policy Statement. The Commission must assume the provider's practices are consistent with the rights, duties and obligations set out in the contracts. Why else would the terms be in the contract? The Commission must enforce the "entitlements" by declaring any practice (whether in a contract or not) that is inconsistent with the Policy Statement practices is contrary to public policy, void, unenforceable and inherently deceptive, meaning consumers can enforce their FCC "entitlements" using state contract and/or deceptive trade practice laws. The Commission, of course, is also free to take action on its own.

D. Customer privacy is at risk.

Broadband providers' TOS/AUP and current plans entail a massive invasion of customer privacy and destruction of private, confidential and protected information. Communications security is at risk. Almost every broadband provider reserves the right to monitor the content of customers' communications. They claim the right to read everyone's mail, know what is in every file sent or received over their network and hear every VoIP conversation. They say they can store that information and use it as they wish. Although they purport to restrict dissemination outside their organization, they make few promises about what will be done with this information within the organization.

These TOS/AUP can determine the rights of third parties that are not the provider's customers. The rights asserted by the providers apply to information sent to a broadband customer by others. AT&T's DSL terms, for example, provide, in pertinent part:

> AT&T does not pre-screen Content, but AT&T and its designees shall have the right (but not the obligation) to monitor any and all traffic routed though the Service, and in their sole discretion to refuse, block, move or remove any Content that is available via the Service.

AT&T's privacy policy also asserts that AT&T has the right to monitor usage, inspect content and use customers' information as a "business record." Assume an AT&T DSL customer communicates with her counsel on matters related to a workers' compensation dispute in which AT&T is a party. AT&T has the right to monitor all her communications. It can keep a copy of the communications. It can open file attachments, including privileged attorney-client communications from her counsel. One could cogently argue that the contract between the customer and AT&T grant an

unqualified right to monitor and therefore operates as a waiver of all expectations of privacy and hence the privilege.

Data Foundry is not necessarily suggesting that AT&T routinely inspects confidential communications at present. But they reserve the right to do so, and as shown below, they will soon start doing so. The TOS/AUP/Privacy Policies on their face eliminate any reasonable expectation of privacy because the customer consents to inspection and use by the provider. A third party seeking access to private information could point to those terms and thereby secure a judicial ruling of waiver.

Broadband users transmit many kinds of information they want to keep secret for a lot of different reasons. It could be financial or medical information. It could be trade secrets, privileged attorney/client communications, discussions between spouses, priest and penitent conversing about sins and absolution, or any number of privileges protected by law. Back when this was common carriage there was little concern about the provider accessing content and users could reasonably assume the content of their communications would not be monitored. Taking this out of the common carrier regime, however, has (perhaps inadvertently) given rise to the risk that massive amounts of privileged, confidential and private information may be subject to disclosure merely because it is transmitted over the Internet and the TOS/AUP expressly grant consent to monitor, track and use the content of all communications traversing the network.[4]

[4] When a Commissioner's aide sends a draft working paper containing advice and recommendations to the Commissioner from her home computer, is it still protected from disclosure if the Commissioner's contract with the broadband provider grants an unlimited right to monitor, store and maintain the content of all communications? Is the content of a broadband communication no longer protected because it has been knowingly and voluntarily disclosed? *Compare United States v. Miller*, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976) [content of bank records voluntarily disclosed to bank as part of commercial arrangement; no reasonable expectation of privacy] *with Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220

E. It is about to get worse.

Most broadband providers are planning to implement and use Deep Packet Inspection and systems like IP Multimedia Subsystems (or the DOCSIS equivalent). AT&T, for example, hopes to begin using IMS this year. These capabilities inherently involve intense scrutiny of envelope information and content, including – among other things – the source and destination, and the devices and applications/services being used. IMS and DPI use this information – after applying provider-supplied criteria – to decide whether to allow use of network resources, the scope of the allowance, the priority to assign, and, of course, to enable "fine-scale charging" for different uses since the open, flat-rate Internet will have been relegated to the dust-bin of history. The providers plan to massively invade and destroy privacy and security of confidential information.

Attachment B provides a more detailed discussion of Deep Packet Inspection and the privacy/security implications of its use in association with broadband.

F. What the Commission should do.

1. Recognize customers' "entitlement" to not be "disentitled" from control over their confidential information. Customers own their information. It is their property, and they have the right to maintain dominion over and control disclosure of, their information. The broadband providers' current TOS/AUP and Privacy Policies and their plans to use Deep Packet Inspection threaten this dominion and control because the user will no longer have a reasonable expectation of privacy as a result of contractual

---

(1979) [pen register records numbers dialed, which are knowingly and voluntarily conveyed to phone company] *and Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967) [reasonable expectation of privacy to "content" of communication, since not voluntarily disclosed to third parties, including phone company].

consent to inspection and use of this information, including content. It is imperative that customers be allowed to use broadband to transmit confidential information without fear that privacy/confidentiality and security will be compromised by virtue of their contract with providers or the actions of the providers.

2. Declare any contract provision or practice inconsistent with the Policy Statement (as supplemented) is contrary to public policy and therefore unreasonable, unenforceable and inherently deceptive. Hold consumers will be able to enforce their entitlements pursuant to state law, similar to the result when the Commission detarrifed nondominant carrier services.[5]

This would be consistent with the notion that broadband is competitive (although it is not). The Commission has decided it should not be subject to federal regulation under the common carrier regime. Therefore, it has to be treated in the same way as all consumer contracts, and dealt with through normal state contract and deceptive trade practice laws. The Commission can declare where the public interest lies, as it did in the Policy Statement. Unless the resulting application of state consumer contract law is clarified, the providers will argue state law cannot apply because of pre-emption and primary or exclusive jurisdiction with the Commission, but they will also argue that the

[5] Second R&O, *In the Matter of Policy and Rules Concerning the Interstate, Interexchange Marketplace, Implementation of Section 254(g) of the Communications Act of 1934, as amended*, CC Docket No. 96-61, FCC 96-424, ¶¶5, 21, 27, 38, 11 FCC Rcd 20730, 20733, 20742-43, 20746-47, 20750-51 (rel. Oct. 1996) ["Moreover, when interstate, domestic, interexchange services are completely detariffed, consumers will be able to take advantage of remedies provided by state consumer protection laws and contract law against abusive practices."]; *aff'd MCI Worldcom, Inc. v. FCC*, 209 F.3d 760. 765 (D.C. Cir. 2000) ["Moreover, as we read the Commission's decision the essence of its reasoning was a desire to put the interexchange carriers under the same market conditions as apply to any other nonregulated provider of services in our economy."]

Commission has no enforcement powers. An “entitlement” is a right that can be enforced. These providers want deregulation, but they also want to be protected from the normal rules for contracts in unregulated areas of commerce. That is not an “entitlement” they deserve.

G. Conclusion.

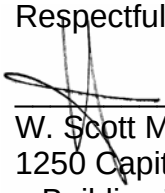
The Commission needs to quit pretending that broadband competition is vibrant, this imaginary competition will adequately protect consumer interests and common carrier like regulations are not necessary or appropriate. The Internet exists today only because the telephone companies could not commit infanticide during the 1980s and early 1990s – because of the very common carrier principles that are now gone.

The dominant broadband providers cannot claim any of the credit for the extraordinary success of the Internet. Others made it what it is, despite – not because of – incumbent telco and cable companies’ early lack of attention and later attempts to limit its growth and potential as a means to communicate. The incumbents know that the only way they can control it is through their power over access to the infrastructure on which it runs. They intend to monetize the Internet by changing the access business model from open and flat-rated to closed and metered, with “fine scale” charges depending on the perceived value derived from the application/service/device being used. While these companies do have a reasonable expectation of a return on their investment, they cannot be allowed to leverage their control over the transmission “market” into the separate application, IP services, devices and content markets. Customers’ privacy and security should not be sacrificed merely so the providers can actualize their forthcoming metered billing plans.

The Commission asked in the NOI whether broadband providers are complying with the Policy Statement. They are not. The Commission asked if the Policy Statement was sufficient. It is not. While the Policy Statement is toothless and inspirational at best, it is at present all we have. Please make it better, not worse.

The Commission issued the Policy Statement bestowing empty "entitlements" with one hand the same day it eliminated substantive, meaningful consumer rights with the other hand. The Commission must demonstrate this was not just a sham. If common carrier regulation is gone for good, then declare that any practice, policy or contract term that is inconsistent with the Policy Statement (as supplemented) is unreasonable, unenforceable and inherently deceptive, and these "entitlements" are enforceable through contract actions and deceptive trade practice claims in state court.

Respectfully Submitted,



W. Scott McCollough
1250 Capital of Texas Hwy South
Building Two, Suite 235
Austin, TX 78746
512.888.1112
wsmc@smccollough.com
Counsel for Data Foundry, Inc.

ATTACHMENT A

Telco and CableCo TOS/AUP violate the "entitlements" set out in the Policy Statement

TIME WARNER

Time Warner prohibits open WiFi, file sharing through Peer to Peer Communications and access to corporate networks through telecommuting:
TOS http://help.twcable.com/html/twc_sub_agreement2.html[6]

4. Use of Services; TWC Equipment and Software
…
(b) I agree that the Services I have requested are residential Services, offered for reasonable personal, non-commercial use only. I will not resell or redistribute (whether for a fee or otherwise) the Services, or any portion thereof, or charge others to use the Services, or any portion thereof. Among other things:
…
(iii) If I receive HSD Service, I agree not to use the HSD Service for operation as an Internet service provider, for the hosting of websites (other than as expressly permitted as part of the HSD Service) or for any enterprise purpose whether or not the enterprise is directed toward making a profit. I agree that, among other things, my use of any form of transmitter or wide area network that enables persons or entities outside the location identified in the Work Order to use my Services, whether or not a fee is sought, will constitute an enterprise purpose. Furthermore, if I use a wireless network within my residence, I will limit wireless access to the HSD Service (by establishing and using a secure password or similar means) to the members of my household.

6. Special Provisions Regarding HSD Service
…

(e) Use of ISP and OLP Service. I agree that TWC and/or my ISP and/or OLP has the right, but not the obligation, to edit, refuse to post or transmit, request removal of, or remove or block any material transmitted through, submitted to or posted on the HSD Service, if it determines in its discretion that the material is unacceptable or violates the terms of this Agreement, any TWC consumption limits or any other Terms of Use. Such material might include personal home pages and links to other sites. In addition, I agree that, under such circumstances, TWC may suspend my account, take other action to prevent me from utilizing certain account privileges (e.g., home pages) or cancel my account without prior notification. I also agree that TWC and/or ISP and/or OLP may suspend or cancel my account for using all or part of the HSD Service to post content to

[6] While not directly relevant to the principles, it is worth noting that Time Warner requires its customers to waive any right to complain if Time Warner violates the FCC's rules prohibiting deceptive descriptions of its taxes, fees and surcharges and outlawing using USF passthroughs as profit centers. *See* Time Warner TOS ¶2(k); compare with 47 C.F.R. §54.712(a). Time Warner's interconnected VoIP service is subject to federal USF. The Commission should hold that such adhesive waiver terms are unreasonable and unenforceable.

the Internet or to engage in “peer to peer” file exchanges or other forms of file exchanges that violate this Agreement or the Terms of Use.

COX CABLE

Cox Acceptable Use Policy and Terms of Service prohibit open WiFi hotspots, Network Address Translation devices (routers), and applications that perform as a server:
AUP https://www.cox.com/policy/#Acceptable_Use_Policy:

Prohibited Activities. You may not use the Service in a manner that violates any applicable local, state, federal or international law, order or regulation. Additionally, You may not use the Service to:
…
Resell or redistribute the Service to any third party via any means including but not limited to wireless technology.

5. Commercial Use. The Service is designed for personal use of the Internet and may not be used for commercial purposes. You may not resell or otherwise charge others to use the residential Service. You agree not to use the Service for operation as an Internet service provider, or for any other business enterprise, including, without limitation, IP address translation or similar facilities intended to provide additional access.
6. Servers. You may not operate, or allow others to operate, servers of any type or any other device, equipment, and/or software providing server-like functionality in connection with the Service, unless expressly authorized by Cox.

COMCAST

Comcast prohibits open WiFi, Network Address Translation devices (common in most routers used for LANs), file sharing, and access to corporate networks through telecommuting:
Terms of Service http://www.comcast.net/terms/use.jsp:

Prohibited Uses and Activities
Prohibited uses include, but are not limited to, using the Service, Customer Equipment, or the Comcast Equipment to:
…
ix. resell the Service or otherwise make available to anyone outside the Premises the ability to use the Service (i.e. wi-fi, or other methods of networking), in whole or in part, directly or indirectly, or on a bundled or unbundled basis. The Service is for personal and non-commercial use only and you agree not to use the Service for operation as an Internet service provider or for any business enterprise or purpose, or as an end-point on a non-Comcast local area network or wide area network;
x. connect multiple computers behind the cable modem to set up a LAN (Local Area Network) that in any manner would result in a violation of the terms of this Policy or an applicable Service plan;
…

xiv. run programs, equipment, or servers from the Premises that provide network content or any other services to anyone outside of your Premises LAN (Local Area Network), also commonly referred to as public services or servers. Examples of prohibited services and servers include, but are not limited to, e-mail, Web hosting, file sharing, and proxy services and servers;
…
xx. connect the Comcast Equipment to any computer outside of your Premises;

Comcast also reserves the right to monitor the content of communications and to block content it finds objectionable for any reason:
Inappropriate Content and Transmissions
Comcast reserves the right, but not the obligation, to refuse to transmit or post and to remove or block any information or materials, in whole or in part, that it, in its sole discretion, deems to be offensive, indecent, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful. Neither Comcast nor any of its affiliates, suppliers, or agents have any obligation to monitor transmissions or postings (including, but not limited to, e-mail, newsgroup, and instant message transmissions as well as materials available on the Personal Web Pages and Online Storage features) made on the Service. However, Comcast and its affiliates, suppliers, and agents have the right to monitor these transmissions and postings from time to time for violations of this Policy and to disclose, block, or remove them in accordance with the Subscriber Agreement and any other applicable agreements and policies.

AT&T

AT&T prohibits “open” WiFi hotspots, use to support VoIP, and applications that perform as a server.

TOS: http://sbc.yahoo.com/terms/
b. SBC Yahoo! DSL and SBC Yahoo! High Speed Internet U-verse Enabled. Your SBC Yahoo! Member Account allows for one broadband connection and one other simultaneous network connection (such as a dial-up line) for a total of two (2) simultaneous network connections to the Internet. SBC reserves the right to prohibit any additional simultaneous network connections. This policy does not prohibit multiple, private users from connecting to the Internet as allowed under these TOS over the same network connection using customer premise equipment such as a router or home networking equipment. Public Use connections are prohibited. For purposes of these TOS, Public Use means unrestricted, open, communal or shared use by third parties unrelated and/or not affiliated to the Member either for profit or not for profit (referred to herein as “Public Use”).
...
IP Addresses.SBC Yahoo! DSL and SBC Yahoo! High Speed Internet U-verse Enabled Services are provided with either a dynamic Internet Protocol (“IP”) address, a static IP address, or multiple static IP address service (as applicable) at SBC’s sole discretion. The dynamic IP address is a single Internet address intended for use with a single Member Account and any associated Sub Accounts. The static IP address or multiple static IP address service is intended for use with a single computer or a network of

computer/servers. You may not use the Service in a manner that is inconsistent with these intended uses. Except to the extent that you have selected the technician installation option when ordering Service, SBC Yahoo! is not responsible for providing support for the installation of any customer premise modem or router with your Service, and in no event will SBC Yahoo! be responsible for any ongoing maintenance or management of any customer premise modem or router with such Service. SBC Yahoo! is also not responsible for providing assistance in the configuration of a local area network with your SBC Yahoo! Service. Primary and secondary domain name service is only provided as part of the static IP address or multiple static IP address service through SBC Yahoo! DSL. In the event you are assigned a static IP address or multiple static IP addresses, the specific IP address(es) assigned shall be at SBC's discretion, and SBC reserves the right to change such IP address assignments at any time.

RESTRICTIONS ON USE AND PROHIBITION OF RESALE
No Resale.
The Service is provided for your use only (unless otherwise specifically stated) and you agree not to reproduce, duplicate, copy, sell, transfer, trade, resell or exploit for any commercial purposes your membership in the Service, any portion of the Service, use of the Service, or access to the Service, including, but not limited to, reselling capabilities enabled or used by a specific application (including, without limitation, Voice Over Internet Protocol (VOIP)). All aspects of the Service, except that portion provided by third party providers, is copyrighted and property of SBC and/or Yahoo! as applicable. The Service is intended for access to and use of electronic mail, Usenet newsgroups, Internet relay chat, the Internet and any other proprietary or non-proprietary services that SBC Yahoo! makes available to its Members.

Restricted Use.
You agree not to permit anyone else to use your Member Account and that each Sub Account may only be used by one member of your household or business. You agree that the Service is not to be used to host peer-to-peer applications that you are not actively using. You agree that the Service is not to be used to trunk or facilitate public internet access ("Hotspots") or any other Public Use of the Service, except for FreedomLink.

TOS: http://www.att.net/general-info/terms-dsl-data.html#useserv

Terms and Conditions
AT&T DSL SERVICE
SUBSCRIBER AGREEMENT
Effective Date - March 2007

…
1. ACCEPTANCE OF TERMS

Welcome! Thank you for choosing AT&T DSL Service as your gateway to the Internet and enjoying the benefits of the AT&T Worldnet® Service Web Site. We know you're eager to begin using your Service, but before you do we encourage you to familiarize yourself with this Subscriber Agreement. This material, including all

information found in the registration process, is the agreement that will apply to your use of the Service.

By enrolling in, using, or paying for the Service you confirm your agreement to these terms and conditions as well as your acceptance of the changes we make to the agreement. If at any time after you have read the Subscriber Agreement and all of its components you do not agree to be bound by the Subscriber Agreement, you should immediately exit registration, end your use of the Service, or cancel your account. Thank you again for relying on AT&T.

In this Agreement ("Agreement"),
"You/Your" means any member or other person or entity using the Service or any part of the Service, including, but not limited to, using the AT&T Worldnet Web Site and the information or features offered in or through the AT&T Worldnet Web Site.

…

To qualify to purchase AT&T DSL Service, you must register for AT&T Worldnet Service as your Internet Service Provider.

…

4. AT&T'S ONLINE PRIVACY POLICY

As an AT&T DSL Service member, you give us information about yourself that we use to conduct our daily business with you. With AT&T's Online Privacy Policy we want to assure our members that we keep such customer-identifiable information as confidential as possible. To view AT&T's Online Privacy Policy go to http://www.att.com/privacy.

…

Eligibility
To become a member of AT&T DSL Service you must have AT&T Worldnet Service as your Internet Service Provider and you have to be at least eighteen years old. You must register using your own name. If you use a credit card for payment, you must provide a credit card account number which is issued in your name or which you are authorized to use.

…

E-mail I.D.
… You may not transfer or permit people outside your household to use your Service account.

…

a. Improper Use. You agree to comply with the "ABCs of AT&T Worldnetiquette," which are described in Section 10. You cannot create a network (whether inside or outside of your residence) with AT&T DSL Service using any type of device, equipment, or multiple computers unless AT&T has granted you permission to do so and you use

equipment and standards acceptable to AT&T. AT&T may cancel, restrict, or suspend the Services and this Agreement under Section 11 below for violating these provisions.

b. Residential Use Only. You agree that the Services will be used exclusively for personal, residential use and not for use in a commercial, small or home business use.

…

10. ABCs OF AT&T WORLDNETIQUETTE

To maintain an informative and valuable service, AT&T has established the ABCs of AT&T Worldnetiquette. While it is not our intent to control your online communication or monitor its content, we may edit or remove content that we become aware of and determine to be harmful, offensive or otherwise in violation of these ABCs. Violation of these ABCs may also result in the termination or suspension of your account. These ABCs apply to all content provided to or through the Service, including e-mail messages, newsgroup postings, chat, and personal web pages.

…

b. Monitoring and Removal of Content. AT&T does not pre-screen Content, but AT&T and its designees shall have the right (but not the obligation) to monitor any and all traffic routed though the Service, and in their sole discretion to refuse, block, move or remove any Content that is available via the Service. Without limiting the foregoing, we shall have the right to remove any Content that violates this Agreement or is otherwise objectionable. You agree that you must evaluate, and bear all risks associated with, the use of any Content, including any reliance on the accuracy, completeness, or usefulness of such Content. In this regard, you acknowledge that you may not rely on any Content created by us or submitted to us.

c. Investigation of Unlawful Conduct. AT&T cooperates fully with federal and state enforcement officials investigating unlawful behavior on AT&T DSL Service's system, and members are required to do the same. You acknowledge and agree that AT&T may preserve Content and may disclose Content if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (1) comply with legal process; (2) enforce this Agreement; (3) respond to claims that any Content violates the rights of third-parties; or (4) protect the rights, property or personal safety of AT&T, its users, and the public.

Privacy Policies:
AT&T's Privacy Policies as amended June 16, 2006 (http://helpme.att.net/article.php?item=8620; http://att.sbc.com/gen/privacy-policy?pid=2506; http://att.sbc.com/gen/privacy-policy?pid=7666#3) authorize monitoring and collection of customers' use of applications and content.

AT&T's "privacy policy" covers customer-specific information related to consumption of AT&T communications products, including Internet access and VoIP. AT&T's privacy policy requires Internet customers to consent to AT&T's ownership of

their account information and authorizes AT&T to track and monitor customer usage and maintain that information as a "business record." The policy eliminated a prior express reference stating that the company "does not access, read, upload or store data contained in or derived from private files without the member's authorization." AT&T's policy allows AT&T to engage in deep packet inspection and look at source, destination, sponsorship and the content of the subscriber's information. AT&T reserves the right to exercise dominion and control of that information just as it would any "business record." *AT&T Revises Privacy Policy, Says It May Share Personal Data*, Dionne Searcey, The Wall Street Journal, June 22, 2006.

ATTACHMENT B

Deep Packet Inspection and Associated Subsystems used to implement tiering will violate customer privacy and compromise the security of confidential information.

IP Multimedia Subsystem ("IMS") is a systems definition originally devised to support 3G mobile networks that was later adapted to support fixed networks as well. An industry forum called 3G.IP developed the initial version, and subsequent versions have been handled by the "3rd Generation Partnership Project (3GPP)." A number of vendors have developed systems for sale to broadband providers that incorporate and use IMS. IMS is the leading candidate for the method broadband service providers will use to efficiently capture and track customer usage information as part of their implementation of tiering. While IMS is not a stand-alone product in that it requires other system operation and management tools, it is an example of means broadband providers will use to look at and determine how to treat (and bill for) customers' specific uses of broadband services. It can determine what application, service or device a customer is using, and it can allocate or deny resources (*e.g.*, bandwidth and/or priority) based on these and other provider-selected criteria. More important, it uses "deep packet inspection" to intrusively capture, track and store the content of broadband customers' communications.

Cisco's description of its IMS product makes it fairly clear that IMS can be used to track, limit and control customer choice in several ways – so as to limit "revenue leakage":

> The profitability of appeal of IMS for service providers lies in its ability to provide a standard platform to respond rapidly to marketplace dynamics of revenue decline and the need to better address service personalization (for example, self subscription, buddy lists, etc.) and control (for example, quality of service [QoS], class of service [CoS], charging, security, content filtering, etc.).
>
> •••
>
> •Who? Who are the users-what device and services are they trying to access? More subscriber detail may be provided depending on the service provider's specific needs.
> •What? What are subscribers allowed to do? What is the policy directing the delivery of the service? What timeframe can they do it in? For example, if a customer access a service during peak times, should the customer be charged for it?
>
> •••
>
> •Track transactions by content type, device, or subscriber.
>
> •••
>
> The Cisco SEF is critical to moving from a data highway to a data "toll way" – in other words moving from a basic "highway" service structure to a "toll-way" service structure that allows service providers to reap the benefits of their infrastructure investment by establishing more granular

> levels of visibility and control over subscriber access, usage and location, allowing them to effectively manage, charge and differentiate their unique voice, data, video, or mobile service offerings… The ability to identify subscribers and classify applications on the IP network ensures that services such as VoIP, VoD, and interactive gaming can be prioritized to meet applications metrics differentiating them from current capabilities of "best-effort" networks, thereby helping to ensure price premiums.
>
> •••
>
> By tracking all IP traffic flows and performing stateful deep packet inspection, the solution collects statistics on the applications and services used by individual subscribers.

http://www.cisco.com/en/US/netsol/ns549/networking_solutions_white_paper0900aecd80395cb0.shtml

The Business Communications Review published an article on June 15, 2005 written by John Waclawsky called "IMS 101: What You Need to Know", available at http://www.bcr.com/carriers/public_networks/ims_101_what_need_know_now_20050615 14.htm. The description of the purposes for and capabilities of IMS reveal the purpose for and planned use of IMS:

> The Dusseldorf meeting didn't actually specify any IMS functions, but served to kick off the IMS specification effort, confirming the telcos' twin objectives: to avoid the commodity fate of becoming "bit haulers" and to cash in on the Internet. IMS was expected to satisfy those objectives.
>
> •••
>
> What all these providers have in common is a desire to bring packet-based voice, data and video to their subscribers in such a way that they can control and charge for those services.
>
> •••
>
> IMS is part of a huge 3G gamble by the mobile telephony operators around the world, with assistance from traditional telephony vendors, to obtain control of the vast new Internet medium and monetize it.
>
> •••
>
> This is the emerging, consensus view: That IMS will let broadband industry vendors and operators put a control layer and a cash register over the Internet and creatively charge for it. It is this monetization of the Internet that makes IMS extremely appealing to all communications operators and all but guarantees that it, and its numerous derivatives, are likely to spread.

AT&T selected Lucent as its IMS vendor in October 2005 (http://att.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=21842) and recently announced (http://www.att.com/gen/general?pid=8385) that deployment will occur in 2007. Here is what Lucent published about this product and its use:

> Managing User Access to IMS Services From a services perspective, security begins with identifying and allowing access to services based on end-user credentials. From network login, through accessing a multitude of IMS applications and services, fully centralized Authentication, Authorization and Accounting (AAA) to identify and control users is absolutely critical.

http://www.usipv6.com/6sense/2005/jul/Lucent_6sense_July_2005_Article.pdf.

> IMS cost-effectively enables service providers to deliver blended lifestyle services, positioning the operator to 'own' the customer, regardless of how they access the network.
>
> •••
>
> Enabling development of more personalized, flexible, blended services must start with stripping away complexity. The IMS service vision centers on products, services and software integrated across three layers of the network – the transport layer for end-user access, the services control layer to manage the network, and an applications layer to rapidly deploy new services.

http://www.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=Brochures/MakingIMSSimple_Brochure.pdf.

The broadband industry is rapidly moving to leverage their control over transmission links within the "last mile" – through use of the so-called "services control layer"[7] – to be able to "manage the end-customer experience to achieve full revenue potential." The telephone companies and cable companies want to institute the kind of broadband control at all layers now exerted by the licensed wireless companies. They intend to "monetize the Internet" by "creatively charging." They are not content to provide simple broadband gateway access that allows customers to experience the Internet "digital highway"; they insist on turning it into a "toll-road" with differential charges depending on the "value" the customer is perceived to receive from the service, application, device or content, even though the broadband providers often have nothing to do with that value other than being one of several gateways along the way.

The most disturbing aspect of these plans is the complete loss of privacy and confidentiality that customers will suffer. These providers do not seem to be concerned that deep packet inspection yields and reveals some of the most personal and proprietary information customers have. They believe that they have the right to open packets and inspect and store the contents. They think that if they restrict further dissemination of the information to third parties then they are protecting privacy.

Customers increasingly rely on IP enabled services to perform essential functions and to exchange confidential, proprietary and privileged information. Lawyers communicate with clients and other lawyers through email, and they exchange

[7] Data Foundry is not sure where this newly minted "layer" fits in the OSI or TCP/IP stacks.

privileged information.[8] Businesses exchange confidential documents subject to non-disclosure agreements or for which confidentiality is mandated by statutes (*e.g.*, HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley) both during negotiations and as part of their ongoing relationships with vendors and customers.

Businesses use IP Enabled services, applications and devices as an integral part of e-commerce. They communicate with their vendors, customers, and the government over digital IP networks. Most have no connection to the "content" industry. They are not Google, YouTube, FaceBook or Yahoo. They are not in the communications business at all but they are totally dependent on their communications investment and practices to operate their trade. AT&T, Qwest, Cox and Comcast have no basis to demand the right – for the first time – to so deeply intrude into the extraordinarily proprietary and confidential information that these businesses and those that communicate with them exchange using IP Enabled services, devices and applications.

Broadband providers AUP/TOS/Privacy Policies, in combination with Deep Packet Inspection, allow intrusive monitoring of the content and information customers transmit or receive. This contractual and technical capability interferes with and may well eliminate all sorts of privileges presently recognized under law and it could put companies at risk in terms of compliance with specific congressional dictates or nondisclosure agreement obligations to keep certain information confidential. Broadband service providers have no justifiable reason to capture this information.

These policies will frustrate compliance with legal obligations, will lead to disclosure of trade secret information, will unreasonably invade the privacy rights of both individuals and companies and will inevitably increase the cost of business since the affected entities will have to take additional and costly measures to try to prevent disclosure.

[8] There is some debate over the extent to which attorneys need to take special measures, such as encryption, to protect attorney-client communications. *See*, Joshua M. Masur, *Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail*, 14 Berkeley Tech.L.J. (1999), http://btlj.boalt.org/data/articles/14-3_fall_1999_9-masur.pdf. One significant problem, however, is that the telco or cable company is likely to be serving the client who may not know how or for some reason may not be able to encrypt communications with counsel. The broadband provider will be able to intercept and look at the confidential information sent by a client to the attorney and this kind of disclosure may well operate to destroy any attorney-client privilege. The broadband provider may choose to block or impede encrypted information if the client tries to maintain confidentiality.

Federal Communications Commission

The FCC Acknowledges Receipt of Comments From …

Data Foundry, Inc.

…and Thank You for Your Comments

Your Confirmation Number is: '2007615414111 '

Date Received: Jun 15 2007

Docket: 07-52

Number of Files Transmitted: 1

DISCLOSURE

This confirmation verifies that ECFS has received and accepted your filing. However, your filing will be rejected by ECFS if it contains macros, passwords, redlining, read-only formatting, a virus or automated links to source documents that is not included with your filing.
Filers are encouraged to retrieve and view their filing within 24 hours of receipt of this confirmation. For any problems contact the Help Desk at 202-418-0193.

Initiate a Submission | Search ECFS | Return to ECFS Home Page

FCC Home Page | Search | Commissioners | Bureaus/Offices | Finding Info

updated 12/11/03