Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

February 28, 2007
Maureen Ohlhausen
Director
Office of Policy Planning
Federal Trade Commission
445 12th Street, SW
Washington, DC 20554

RE: "Broadband Connectivity Competition Policy Workshop - Comment, Project No. V070000"

Dear Ms. Ohlhausen,

Thank you for hosting the FTC Internet Access Task Force Workshop "Broadband Connectivity Competition Policy" or as we call it "*Consumer Choice in the Applications they use in Association with Broadband*."

I appreciated the opportunity to speak before the panel and I would like to use this opportunity to provide the outline printed materials that I used for reference for my talk.

Kind Regards,

Ronald B. Yokubaitis
Chairman
Data Foundry, Inc.

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

I. INTRODUCTION

Data Foundry, Inc. was established in 1994 and has its headquarters in Austin, Texas. Data Foundry provides Disaster Recovery, Data Center Outsourcing, Managed Data Center, and Business Continuity Work-Site Recovery Services. We own and operate regionally-dispersed, secure Data Center and Work-Site Recovery facilities which provide 24x7x365 support from state-of-the-art Network Operation Centers. As a global provider of managed services, 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 are currently utilizing our solutions. They include companies and others that have traditional privileges, contractual nondisclosure agreements and statutory obligations to maintain confidentiality of corporate, governmental and individual consumer/citizen proprietary information.

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, and often through the Internet. Many customers buy high capacity IP connections for the sole or primary purpose of accessing information they store on their servers co-located at a Data Foundry Data Center there connected to the Public Internet. To do so 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 either 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 a physical layer operator chose to impose service "tiers" 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 also suffer from degraded or limited access if physical layer providers were allowed to 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, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

II. IMS DETAILED

IMS is the tool that will be used to implement tiering, and is a mechanism for destruction of privacy and security

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 the means broadband providers will probably 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 customer's 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

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

> 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_2005061514.htm. Their description of the purposes for and capabilities of IMS are more revealing and up-front about 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.

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

AT&T selected Lucent as its IMS vendor in October 2005. http://att.sbc.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=21842. Here is what Lucent says about its 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.lucent.com/livelink/0900940380094f50_Product_news_bulletins.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.lucent.com/livelink/090094038008b683_Brochure_datasheet.pdf

These materials make it absolutely clear that the broadband industry is rapidly moving to leverage their control over the transport layer – through use of the so-called "services control layer"[1] – 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.

Perhaps what is most disturbing is the complete loss of privacy and confidentiality that customers will suffer as a result of these providers' plans. These providers do not seem to be concerned that their

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

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

deep packet inspection will yield and reveal 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 privileged information.[2] 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 of these business 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.

AT&T's recent Privacy Policy in combination with its IMS-based ability to perform deep packet inspection and monitor the content and information customers transmit or receive interferes with and may well eliminate all sorts of privileges presently recognized under law and it could put companies at risk in

---

[2] 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.

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

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.

III. EXISTING TOS/AUP POLICIES VIOLATE NET NEUTRALITY AND THREATEN CUSTOMER CHOICE IN THE INTERNET BROADAND APPLICATIONS THEY USE

Telco and CableCo TOS/AUP and Privacy Policies allow inspection and wide use of customer content and prohibit telecommuting, VPNs, LANs, open WiFi and file sharing

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

COX CABLE
Cox Acceptable Use Policy and Terms of Service prohibit open WiFi hotspots, and applications that perform as a server.
https://www.cox.com/policy/#Acceptable_Use_Policy

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. Comcast also reserves the right to monitor the content of communications and to block content it finds objectionable for any reason.
http://www.comcast.net/terms/use.jsp

AT&T
AT&T prohibits “open” WiFi hotspots, use to support VoIP, peer to peer file sharing and applications that perform as a server.
http://sbc.yahoo.com/terms/

AT&T’s Privacy Policies as amended June 16, 2006 (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

Data Foundry, Inc.

1044 Liberty Park Dr.
Austin, Texas 78746
Tel: (512) 684-9700
Fax:(512) 684-9701
http://www.datafoundry.com

of applications and content. AT&T's new "privacy policy" covers customer-specific information related to consumption of AT&T communications products, including Internet access and VoIP. AT&T's privacy policy now 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 new policy also 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 new 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

AT&T has also promulgated additional privacy terms specific to its U-Verse "video" services: http://help.sbcglobal.net/article.php?item=8620

All links visited and content verified February 7, 2007.