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

In the Matter of	)	
	)	
International Comparison and Consumer	)	
Survey Requirements in the Broadband	)	GN Docket No. 09-47
Data Improvement Act	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
Inquiry Concerning the Development of Advanced	)	
Telecommunications Capability to All Americans in a	)	
Reasonable and Timely Fashion and Possible Steps to	)	GN Docket No. 09-137
Accelerate Such Deployment Pursuant to section 706	)	
of the Telecommunications Act.	)	

COMMENTS OF THE NEW AMERICA FOUNDATION – NBP PUBLIC NOTICE #24

Benjamin Lennett
James Losey
Dan Meredith
Robb Topolski
Sascha Meinrath

Open Technology Initiative
New America Foundation
1899 L Street, NW
Suite 400
Washington, DC 20036
oti@newamerica.net

December 14, 2009

SUMMARY

In the present *Notice*, the Federal Communications Commission (FCC or Commission) seeks comment on empowering consumers by ensuring sufficient access to relevant information about fixed residential and small business Internet broadband services. The Commission further seeks comment on measuring, tracking, and reporting service quality of fixed services.

The New America Foundation's Open Technology Initiative (NAF) commends the Commission for this *Notice* and the commitment to empowering consumers and promote transparency in broadband services. NAF believes that existing rules to ensure consumers' access to relevant information about the communication services they are purchasing are grossly insufficient. Voluntary guidelines are insufficient as a substitute for codified regulations, as service providers routinely fail to disclose meaningful information to consumers. Substantial changes to the Commission's existing rules are necessary to remedy these problems and empower consumers with the information they need to make an informed choice of their Internet service provider (ISP) and offering. However the problem goes beyond just the challenges faced by consumers; policymakers, researchers, and innovators have access to too little information about the workings of the Internet. Access to raw data on Internet traffic and performance has substantially diminished as scientists have struggled to conduct network research under ever-increasing constraints.

To remedy these problems, NAF provides the Commission with several policy recommendations including:

- Clear disclosure rules to ensure consumer have access to fundamental information about broadband service offerings.
- Standardized information disclosures across all fixed and mobile broadband services.
- Require advertisements to provide clear expectations of the service offering including the typical capabilities and the actual price of the service, not theoretical maximums.
- Require providers to inform consumers of the FCC complaint process.
- Allow consumers to append test results from measurement tools to complaints filed with the FCC and release complaint data on each provider.
- An FCC led effort to measure and collect fundamental data on broadband service capabilities and Internet performance and traffic statistics.

In addition, these comments provide an overview of both active and passive measurement systems. We encourage the Commission to think broadly about measurements and data collection. The FCC should promote efforts that will empower consumers and the Commission assess the capabilities of broadband services and create viable sources for data on Internet traffic and network performance for researchers and policymakers. Important to the success of these efforts, the FCC should focus on openness and transparency in its measurement process and ensuring access to raw data by the public, researchers and policymakers.

TABLE OF CONTENTS

I. Introduction **4**

II. Consumer Transparency Regarding Fixed Services **6**

1. Information to Potential New Customers **8**

2. Information to Existing Customers **12**

3. Complaint Procedures **13**

III. Measurement of Fixed Services **14**

1. Active Measurement (End-User Initiated Tests) **18**

2. Passive Measurement (Customer Panel Devices) **20**

3. Passive Middle-Mile and Backbone Measurement **22**

IV. Conclusion **24**

I. INTRODUCTION: TRANSPARENCY AND MEASUREMENT OF BROADBAND SERVICES IS VITAL TO THE NATIONAL BROADBAND PLAN AND THE PUBLIC INTEREST

The New America Foundation's Open Technology Initiative (NAF) respectfully submits these comments in response to the Commission's *Public Notice #24* in the above-captioned docket.[1] In the *Notice*, the Commission seeks comment on empowering consumers by ensuring sufficient access to relevant information about fixed residential and small business internet broadband services. The Commission further seeks comment on measuring, tracking, and reporting service quality of fixed services.

NAF commends the Commission for this *Notice* and its commitment to promoting transparency in broadband services. NAF believes that existing rules to ensure consumer's access to relevant information about the communication services they are purchasing are grossly insufficient. Service providers overpromise on the capabilities of their service and routinely fail to disclose limitations to services and hidden fees. This leads to substantial consumer confusion and frustration when choosing among service providers and plans, assessing the actual speeds and quality of a broadband service, and the actual cost of a service. Consumers have limited or no access to a wide range of service aspects, including typical service prices, usage limits and fees, actual performance and imposed limitations, and other contract terms. Voluntary guidelines are not proving sufficient as a substitute for codified regulations, as service providers routinely fail to disclose meaningful information and hide the information they do disclose in fine print below misleading "base rates" and "advertised speeds." Substantial changes to the Commission's existing rules are necessary to remedy these problems. The Commission has clear authority and statutory obligations to strengthen current information disclosure policies, and must act upon these authorities.[2]

These challenges are faced not just by consumers, by also by policymakers, researchers, and innovators who access to little information about the workings of the Internet. Such an information void did not always exist. NSFNET, which served as the precursor backbone to the commercial Internet, collected and made publicly available fundamental performance statistics from 1988 to 1995. Since that time, access to raw data on Internet traffic, topology, routing, and security have diminished, causing Internet researchers have struggled to conduct legitimate and reproducible experiments.[3] Thus, it is important not only for the Commission to bring transparency to consumers, but to pursue efforts to provide access to fundamental information on broadband connections and Internet performance.

The benefits of a focused FCC effort for Internet services are three fold:

---

[1] *Broadband Measurement and Consumer Transparency of Fixed Residential and Small Business Services in the United States*; GN Docket Nos. 09-47; GN Docket Nos. 09-51; GN Docket Nos. 09-137; Notice of Inquiry, (rel. November 24, 2009) ("*Notice*").

[2] *See* para. 5, *Comments of Consumer Federation of America, Consumers Union, Free Press, Media Access Project, New America Foundation, and Public Knowledge*, CG Docket No. 09-158; CC Docket No. 97-170; WC Docket No. 04-36; available at http://fjallfoss.fcc.gov/ecfs/document/view?id=7020141629..

[3] *See* Meinrath, Sascha D. and claffy, kc; *The COMMONS Initiative: Cooperative Measurement and Modeling of Open Networked Systems*, 418; Appendix 1.

- ***Empowering Consumers and Promoting Competition***

As the Commission correctly concluded, "the proper functioning of competitive markets is predicated on consumers having access to accurate, meaningful information in a format that they can understand."[4] Just as the Food and Drug Administration requires food manufacturers to appropriately label products with a list of ingredients and the nutritional information,[5] consumers should be afforded a similar understanding of their broadband offering. In an effort to develop a similar proposal, NAF developed a Truth-in-Labeling disclosure form.[6] A standard form allowing consumer to compare apples to apples among providers is essential to promoting competition in broadband services.

- ***Spurring Research and Innovation***

Obstacles to the collection and analysis of Internet traffic and performance data since the transition to the commercial Internet pose not only formidable technical and engineering challenges, but more daunting legal, logistical, and proprietary considerations. In combination, these issues have left the Internet research community continually struggling to validate research that fosters new network innovations. A FCC-led effort to collect measurements of broadband networks offers an unprecedented opportunity to provide rigorous empirical data against which to validate theory, modeling, and support for scientific research, development of new measurement technology and evaluation of proposed future Internet architectures.[7]

- ***Improving Public Policy***

As the Commission examines complex issues of network congestion and network management, it is entirely dependent on analyses of traffic and usage data from service providers. Given the increasingly critical role of information and communications technologies for national productivity, economic competitiveness, and even security, the costs of policy errors could be grievous. Yet decision makers are often forced to operate in an information vacuum—being placed in the position of only having access to the information that the companies which would be affected by policy and regulatory changes are willing to share.[8] Data that is publicly accessible, and independently verifiable would support public analysis of actual Internet traffic, to inform salient debates on technical, economic, policy, privacy, and social issues relating to the Internet – many of which have been shrouded in secrecy. The data derived from a systemic collection of end-user data and Internet performance and traffic statistics would provide expert agencies with access to vital independent research and analysis.[9]

---

[4] *Second Truth-in-Billing Order* at para. 3.
[5] *See, e.g.*, Nutrition Labeling and Education Act of 1990, Pub. L. No. 101-535, 104 Stat. 2353 (codified as amended in scattered sections of 21 U.S.C.). *See also* Food Labeling Guide, U.S. Food and Drug Administration, http://www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/GuidanceDocuments/FoodLabelingNutrition/FoodLabelingGuide/default.htm (last visited Nov. 4, 2009).
[6] *See* Open Technology Initiative, *Broadband-Trut-in-Labeling*; Appendix 2.
[7] *See The COMMONS Initiative*; Appendix 1.
[8] *Id. See also* Meinrath, Sascha D., *Analyzing in the Dark: The Internet Research Data Acquisition Crisis*, Appendix 6.
[9] *See The COMMONS Initiative*, Appendix 1.

NAF proposes a number of detailed policy recommendations and ideas to the Commission. No matter what specific rules the Commission decides upon, NAF believes the following principles and policies are essential to promoting broadband transparency and measurement:

Consumer Transparency

- *Provider information and disclosures should be prominently displayed, easily accessible and standardized across all fixed and mobile broadband services.*
- *Vital information on broadband service offerings should be available upfront, before the consumer purchases the service.*
- *Prices should reflect the actual price of the service, including but not limited to, the non-promotional price, along with any installation, necessary equipment, taxes and other fees.*
- *Advertisements should provide clear expectations of the service offering including the typical capabilities, not theoretical maximums, and the actual price of the service.*
- *Existing customers should receive advance and explicit notification on any changes to the technical capabilities, terms of service (TOS) or use, privacy policy, network, management practices, and any other changes to the service.*
- *Users should be able to report inconsistencies and file complaints to the FCC if the actual capabilities of their service differ from the capabilities indicated by their service offerings.*
- *Aggregate statistics of those complaints should be publicly available, including the number of complaints and reasons for complaints, per provider.*

Measurement Transparency

- *Sustained FCC-led effort to measure and collect fundamental data on broadband service capabilities and Internet performance and traffic statistics.*
- *Measurement tools should be open source, with an open API, to allow for independent verification of test methodologies and maximum extensibility.*
- *Measurement data, subject to privacy considerations, should be open and publicly accessible.*

II. CONSUMER TRANSPARENCY REGARDING FIXED SERVICES

For a consumer to (1) choose a provider, (2) choose a service plan, (3) manage the use of the service plan, and (4) decide whether and when to switch to an existing provider of the plan, they need to know not only the information that affects the reliability of their use of the service and applications over the service, but have this information easily available and comparable between providers, services, and offers. Consumers need data on four critical aspects of their service: cost of the service, technical capabilities, terms of the service, and the limitations of the service.

Clear disclosure rules are needed to ensure consumer have access to the following:

- Actual service costs, including disclosure of mandatory line-item charges, non-promotional rates, and one-time and recurring fees;
- Limits on usage, as well as standardized and meaningful representations of overage fees;
- Actual, expected speeds of Internet access services in times of peak and non-peak usage, not just theoretical maximums;
- Meaningful information about restrictions and provider rights asserted in the terms of service;
- Meaningful information about actions conducted by providers that monitor, manage or interfere with a subscriber's use of services or Internet traffic; and
- Obstacles to ending or changing service, and their purpose for being imposed, including in early termination fees and device locking mechanisms.[10]

NAF has created a sample Broadband Truth-in-Labeling disclosure, which is detailed below.[11] The intent of the disclosure form is to require ISPs to use a standardized label to inform potential and existing customers about the broadband services they are subscribing to, including technical capabilities, service guaranteed, prices, service limits, and other related elements. The labels aim is to educate customers, make broadband services more transparent, and to spur broadband competition, innovation and consumer welfare. The Broadband Truth-in-Labeling disclosure should be standardized to comprise several typical elements as indicators of broadband service quality, such as minimum expected speed and latency to the ISP's border router (where the ISP connects to the rest of the Internet) and service uptime. These minimum assurances will be supported by the ISP as guarantees in the delivery of broadband services, backed by technical support and service charge refunds or credits. In addition to the description of minimum guarantees of the service, the disclosure should include all applicable fees, a common description of the technology used to provide the services, any service limits such as a bandwidth caps or the application of any traffic management techniques, the length of the contract terms, and specific links to all additional terms and conditions. Requirements should be established for disclosing any highly objectionable or surprising terms such as arbitration restrictions or customer data-selling.

When considering disclosure rules, it is critical for the Commission to recognize the importance of disclosing information that may be currently beyond the understanding of the average consumer. Although some providers would prefer to oversimplify the consumer purchase or comparison of broadband services to simple advertising slogans and "up to" speed consideration, it is important to the public interest that consumers have every opportunity to truly understand a broadband service. For example, although the average consumer currently may have little understanding of the importance or impact of latency on their on-line experience, it does not follow that they will never understand. Rather, just as when the PC was relatively new, most consumers had little recognition of technical considerations such as processor speeds, RAM, or hard disk space, they have become increasingly important to consumers purchasing

[10] *See* p. 21, *Comments of Consumer Federation of America, Consumers Union, Free Press, Media Access Project, New America Foundation, and Public Knowledge*, CG Docket No. 09-158; CC Docket No. 97-170; WC Docket No. 04-36; available at http://fjallfoss.fcc.gov/ecfs/document/view?id=7020141629.
[11] *See Truth-in-Labeling*; Appendix 2.

decisions of PCs as well as software, which often provide consumers with the necessary system requirements before purchase.

In the same way, more advanced technical information and statistics about broadband service offerings will become increasingly relevant to consumers over time. Similar to software companies, application and content developers could provide consumers with the necessary broadband requirements for proper performance. This would help to maximize consumer utility for broadband and allow purchasing decisions to be influenced by performance characteristics relevant to the applications and content consumers demand. In addition, requiring the public disclosure of even complex information would allow for interested individuals and entities to crowd-source the information and improve the ability of consumer groups and publications to develop guides and comparisons. Currently, such organizations have scant information to develop comparisons of broadband plans or providers, often relying on sporadic reviews or speed-tests from ISP customers. The possibilities are endless for the types of information that could be crowd-sourced and reformulated to improve consumer welfare as result of greater transparency.

1. Information to Potential New Customers

As the Commission noted, "To choose a provider, consumers need information on the availability and quality of network services and related equipment (coverage and reliability), various provider fees for similar services, and full disclosure of the contractual commitments they are undertaking. To choose a service, they need to be able to compare and contrast service plans offered by different providers and assess the full costs of each option. To use a service plan well, they need accurate and transparent billing statements, clear usage information, and accurate disclosures about changes in fees or terms of service during the relevant period."[12]

Internet Access Providers should disclose the important facts and details of the broadband offering before consumers purchase service. Providing clear, meaningful, comparable disclosures ultimately spurs competition between ISPs and encourages the future development of new broadband technologies. NAF has already developed an example Truth-in-Labeling standard. Drawn from similar useful disclosure requirements by lenders, these Broadband Truth-in-Labeling disclosure standards could give the marketplace a much-needed tool that clarifies and adds meaning to the terms and conditions of the service being offered.[13] Based on the "Schumer Box" required for loan applications, this standardized format could be used to display the price, features, and limitations of a service offering on a provider's website. This type of display must be included in the initial presentation of a service offering. If a comparable format of service details is not available until a consumer purchases the service, the consumer's ability to compare services or providers is greatly diminished as the consumer must initiate purchase of multiple offerings in order to compare. This Broadband Truth-in-Labeling disclosure must be shown to the consumer as part of the sign-up process and must be assertively presented again any time the ISP decide to alter the terms in such a way that alters the facts on the original Broadband Truth-

[12] *See* ¶ 23, *Customer Information and Disclosure Truth-in-Billing and Billing Format IP-Enabled Services*, CG Docket No. 09-158; CC Docket 98-170; WC Docket No. 04-36, Notice of Inquiry, FCC 09-68 (rel. 28,2009) ("Notice").
[13] *See Broadband Truth-in-Labeling*; Appendix 2.

in-Labeling disclosure. In addition, to the greatest extent possible, these disclosures should be as geographically specific as possible for providers with a national footprint.

Figure 1: NAF Broadband Truth-in-Labeling Form

ExampleCom Ultra 15 Mbps Broadband Truth-in-Labeling	
Advertised Speed	15 Mbps downstream/2 Mbps upstream
Service Guarantees **Services are measured from and to the border router.**	
Minimum Speed at Border Router	8Mbps downstream /384Kbps upstream
Minimum Reliability/Uptime	96%
Maximum Round-trip Latency (Delay) to Border Router	50ms
Service Guarantee Terms	Daily service credit upon request for any outages or extended periods of under-delivery of service
Prices	$44.99 monthly service $19.99 monthly for the first six months on promotion
Service Limits (List all traffic management techniques)	• Exceeding 100GB calendar week considered excessive use, subject to disconnect penalties, see http://www.examplecom.invalid/excessive • Traffic by heavy users in congested areas is artificially slowed, see http://www.examplecom.invalid/shaping
Other Fees (ISPs cannot charge if not listed)	$3 monthly modem rental fee $59.99 installation fee $19 outlet installation $150 early termination during promotion period $2 account change fee $35 service call fee unless $3 monthly inside wiring maintenance plan is in force Sales taxes and franchise fees, vary by location
Contract Term	At will, customer may cancel at anytime after first six months. During the first six months, a cancellation results in a $150 fee.
Service Technology	DOCSIS 1.1 / 2.0 HFC
Legal and Privacy Policies	http://www.examplecom.invalid/legal

a. Vital Information

Technical capabilities

The speed and actual capabilities of broadband service offerings should be a source of competition between services and providers; but in order to be meaningfully comparable, the capabilities represented must reflect the actual performance of the service. Service offering advertisements labeled with the theoretical maximum speed with vague disclaimers such as "up to" or "actual speeds may vary," are completely useless. As the Commission correctly noted the "[m]aximum advertised speed is often cited, but the actual is more useful" particularly since the difference between the median actual speed is often 50% slower than advertised.[14] Consumers must have legitimate information as to the speed of a service offering in order to decide when to switch to a new service or provider. NAF believes a solution to this issue is to require providers to disclose a minimum speed guarantee from a subscriber's connection to a border router or edge

[14] Commission Open Meeting Presentation on the Status of the Commission's Process for Development of a National Broadband Plan, Sept. 29, 2009, Slide 26.

of a provider's network. The minimum guaranteed speed would be determined by the provider and include a measure of reliability. These minimum assurances should be supported by the ISP as guarantees in the delivery of broadband services, backed by service charge refunds or credits if they are not delivered. Such a metric would provide much more useful statistic than the current industry norm of utilizing theoretical maximums, which can vary depending upon location of service, type of day, etc. In addition, other technical characteristics such as latency, a performance characteristic increasingly important for consumers using real-time, two-way communication, should further disclosed.

Service costs

Consumers should know the actual cost of a broadband service. Service advertisements often only present a promotional price for the service whereas the monthly bill will include various fees, surcharges, mandatory bundles, and a monthly rate, which increases after the promotional period ends. These hidden costs obstruct a consumer's ability to accurately compare services and challenge the ability to make informed decisions about switching services. For example, a Verizon mailing advertises a contractual, promotional monthly rate of $19.99 for DSL service, a price that does not include "taxes and fees" or a one-time charge of "up to $55".[15] In order to receive the promotional rate, a customer must also purchase telephone service and after the first six months, the service will increase 60%. Further, if the customer leaves before the contract is up, they will be assess a $79 early termination fee. Verizon also retains the right to increase the cost of the Internet service if a customer cancels the accompanying telephone service.[16]

Early termination fees (ETF) are nearly ubiquitous across all broadband services and are a limitation for users switching services. ETFs are an additional cost burden to switching services on top of any one-time fees a user may be charged when starting a new service. Since they inherently must be taken into account by a consumer when considering changing their service, these charges must be disclosed up front. Similarly complex billing practices need to be disclosed upfront, encompassing the actual monthly costs of a service plan so that a consumer can make an informed decision regarding the costs of different plans. Upfront disclosure to consumers should further include the non-promotional price, along with any and all other fees for the service.

Terms of service

Limited disclosure of terms of service pertaining to Internet services can affect a user's experience on the Internet. As such, this information should be readily accessible, and easily comparable between services and providers. Terms of service for service offerings are often hidden in legal verbiage, small text size, or non-prominent placement compared to other aspects of the service offering.[17] Sometimes, extremely relevant information to the experience of the service, such as a universal declaration that a customer's Internet usage can be monitored or

---

[15] *See* Appendix 3, Exhibit A.
[16] *See Verizon Online Terms of Service*; Appendix 4, Exhibit A.
[17] As noted in *Comments of Consumer Federation of America, Consumers Union, Free Press, Media Access Project, New America Foundation, and Public Knowledge*.

interfered with, can be hidden in the terms of service. For example, Comcast "reserves the right to refuse to transmit or post, and to remove or block, any information or materials" it deems in violation of the acceptable use policy.[18] One network use subject to termination is the distribution of "derivative works...without obtaining any required permission of the owner."[19] Further, Comcast, Quest, and Verizon specify that they may immediately suspend or terminate service if any terms of the Acceptable Use Policy are violated.[20] The privacy practices of the provider are important to be disclosed with the service offering. Consumers need to be informed as to what information about them, and their Internet usage, will be collected through their purchase of the service and what opportunities they have to opt out. For example, Comcast's legal policies reveal that they monitor bandwidth, usage, transmissions, and content.[21] Such practices need to be clearly disclosed to a potential customer.

Limitations

Consumers need to know any limitations that may be applied to the service offering including usage caps, and subsequent overage charges, as well as traffic or network management practices that can influence how a consumer will be able to utilize and interact with the service. If a service offering has a cap on how much data can be consumed within a given period, this must be clear and disclosed up front, along with any fees associated with exceeding the cap. Cap and overage charges must be referenced clearly with any presentation of price (e.g."$40 a month for the first 5GB, $.05 per additional MB.") Any traffic management which may affect a consumer's usage or experience of the service or an application must also not only be disclosed, but this information must be easily accessible before purchase. For example, if the use of certain applications or exceeding a certain amount of bandwidth consumption will result in a lower prioritization of traffic or a different experience of the service, these types of limitations must be disclosed as part of the service offering. With the exception of Comcast, which was compelled to disclose their practices by the FCC,[22] the majority of ISPs have provided relatively little information regarding their network management practices and the capacity limitations of their broadband networks.[23] Even so, in their Acceptable Use Policy, Comcast only offer that they may lower "the priority of traffic for users who are the top contributors to current network congestion."[24] Both consumers and developers would benefit from a *full* disclosure of network management practices with a clear explanation of how the system works. Sufficient disclosure of the network management tools used by ISPs is critical to the designers of Internet applications, as it allows them to predict whether their application will mesh with a given network.[25]

---

[18] *See Comcast Acceptable Use Policy*; Appendix 4, Exhibit B.
[19] *Id.*
[20] *Id., Quest Acceptable Use Policy;* Appendix 4 Exhibit C, and *Verizon Acceptable Use Policy*; Appendix 4 Exhibit D.
[21] *See Comcast Acceptable Use Policy*; Appendix 4, Exhibit B.
[22] *See In re Broadband Industry Practices, Petition of Free Press et al. for Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management,"* Memorandum Opinion and Order, WC Docket 07-52, ¶ 32 (Aug. 20, 2008), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf [hereinafter In re Broadband Industry Practices.
[23] *Id., supra* note 2, at 58 (Comm'r. Tate, dissenting)
[24] *See Comcast Acceptable Use Policy*; Appendix 4, Exhibit B.
[25] *See In re* Broadband Industry Practices, *supra* note 2, app. at 46.

Quality of Service Information

In addition, potential customers would benefit from access to quality of service information on a quarterly or annual basis. Quality of service information could consist of performance and customer service statistics such as average speeds up/down, average latency, jitter, dropped packets, uptime, service outages, and customer equipment failures. Providers should be required to disclose the above quality of service information to consumers on the provider's website.

b. Details in Advertisements

We recognize to a certain extent that the above disclosures and disclosure format may need to vary by advertising format, i.e. television, radio, online, mail, etc. Advertising to consumers needs to provide truthful claims to consumers regarding service offerings. The most vital stats for advertisements are the typical capabilities of a service and the actual cost of service in both print or online and television or radio advertising. For short television or radio advertising spots, providers should clearly indicate that that any "up to" speeds will substantially vary and are not guaranteed. The Commission could also require that providers disclose some measure of actual or typical speeds with a measure of reliability. Alternatively, the minimum guaranteed speed utilized by NAF's Broadband Truth-in-Labeling could be required in the advertisement. Actual prices for services should also be indicated in the ads, including non-promotional pricing, and other fees, along with any usage limits, overage charges, and early-termination fees. Similar requirements should be included for online or mailing advertisements, in easily readable formats and a clear indication of where to view all disclosures about the service – more than simply directing consumer to the provider's website

c. Details at Point of Sale

The point of sale, whether it is a provider's website, over the phone, or any physical sales offices, is the most critical point of disclosure. Providers must be required to disclose any and all information necessary for the consumer to make an informed purchasing decision. Any standardized disclosure forms, such as NAF's Broadband Truth-in-Labeling form, should be prominently displayed on the provider's website before purchase, along with clear links to the complete list of terms of service, fees and limitations. For phone orders, consumers should be provided with same information as available on a provider's website. Paper copies should be provided at any sales offices.

2. Information to Existing Customers

a. Explicit and Clear Communication to Consumers of Any Changes to the Service

Customers must be informed with adequate advance time to any change to terms of service, limitations, or technical capabilities of the service. For example, Comcast makes "reasonable efforts to make customers aware of any changes" to their Acceptable Use Policy, but examples of "reasonable efforts" given are "emailing the customer or posting information on the

Comcast.net website.[26] At a minimum providers, should disclose any of these changes with the bill, either paper or via electronic delivery, if a consumer has opted for that method. The disclosure would explicitly state what about the service has changed, and not require the subscriber to comb through the terms of service or acceptable use policy to determine the changes.

b. Subscriber Tools to Measure Usage

Subscribers should further have access to tracking tools, such as a means to monitor, usage or consumption. As providers have increasingly expressed interest in or implemented usage or bandwidth caps, they have not committed to providing consumers with the necessary information to ensure compliance. Although, companies such as Comcast have offered it would provide subscribers with a tool to monitor their monthly broadband usage, to date suchs tool are still unavailable to subscribers. Over a year after announcing a 250 GB monthly usage cap on subscribers, Comcast has only recently released a "data usage meter" in a pilot program in the Portland, Oregon Area.[27] Even so, it only accounts for a consumer's monthly usage, and provides no means for subscribers to measure their usage in real-time – a significant problem given Comcast's network management system.[28] According to their January 2009 filing with FCC, Comcast's "Fair Share" system de-prioritizes a user's traffic when they exceed 70 percent of their upstream or downstream bandwidth over a fifteen-minute when the network is "Extended High Consumption State."[29] However, Comcast provides the consumer with no means to track their bandwidth consumption, nor is the customer informed that their traffic is being de-prioritized. Such a tool would help consumers understand why a particular application is not working and minimize user frustration. Particularly, given that many of the caps may result substantial overage charges, providers must be required to supply their users with a means to monitor their usage – as they have considerable financial incentives to encourage users to exceed those caps.

3. Complaint Procedures

The current process for reporting service and billing issues with the FCC is insufficient. As the Commission is well aware, a Government Accountability Office survey suggests that many consumers do not know they can submit complaints to the Commission or how they can do so.[30] This is a considerable problem and the Commission should take proactive steps to improve consumer awareness. An immediate step would be to place a link directly to the on-line complaint form more prominently on the FCC website, where currently users have to first click on the consumer link, which takes them to the 'Consumer Bureau' page, where they can then

---

[26] *See Comcast Acceptable Use Policy*; Appendix 4, Exhibit B.
[27] *See* Livingood, Jason, *Comcast Data Usage Meter Launches*; http://blog.comcast.com/2009/12/comcast-data-usage-meter-launches.html.
[28] *See* Letter from Kathryn A. Zachem, Vice President, Regulatory Affairs, Comcast Corp., to Dana Shaffer, Chief, Wireline Competition Bureau, and Matthew Berry, Gen. Counsel, FCC (Jan. 30, 2009); http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6520194593.
[29] *Id.*, p. 7–9.
[30] *See* ¶ 51, *Customer Information and Disclosure Truth-in-Billing and Billing Format IP-Enabled Services*, CG Docket No. 09-158; CC Docket 98-170; WC Docket No. 04-36, Notice of Inquiry, FCC 09-68 (rel. 28,2009) ("Notice").

submit a complaint. Further, the FCC should require providers to include on their bills information how to contact the Commission to file a complaint. In addition, services provider should be mandated to include FCC complaint information on their websites where customer service information is located as well as disclose it to consumers that contact a provider's customer service center by phone or e-mail.

Also, the FCC should consider allowing consumers to append performance test results to the complaint form from measurement tools and to report discrepancies between the actual performance and advertised. As NAF provides below, active measurement tools can empower consumers to test the actual performance capabilities of their broadband connection as well as provide diagnostic tools to determine problems with a broadband connection or why an application is not working. The Commission could even direct consumers on the form to best-practice measurement and diagnostic tools.

In addition, it is critical the FCC make public as much of the complaint data as possible. The current quarterly reports on "Informal Consumer Inquiries and Complaints" are far too limited.[31] The public is only provided with summary statistics on the number of complaints and the top "subjects" for consumer inquiries and complaints. There is no indication of how many complaints and the subject of those complaints for each service provider, although consumers can indicate that on the complaint form. If the complaint process is to have any effect on improving broadband competition and empowering consumers, then the FCC must make publicly available data the number of complaints and the subject of those complaints for each service provider. Such publicly available information could be utilized by any number of consumer groups, publications, or websites to establish consumer comparisons of service providers – giving service provides a clear incentive to improve their customer service. Further, to promote robust analysis of the data, the data should be released in an open format such as .CSV, .ODF, or .TXT, rather than just in PDF form.

III. MEASUREMENT OF FIXED SERVICES

Measuring, collecting, and analyzing data on network performance and traffic has been a hallmark of the Internet. NSFNET, which served as the precursor backbone to the commercial Internet, collected and made publicly available performance statistics from 1988 to 1995. Each of the thirteen backbone nodes (Nodal Switching Subsystems) on NSFNET provided packet, routing control, and statistics gathering (for network traffic information) for the network."[32] NSFNET performance statistics were collected, processed, stored, and publicly reported by the Merit Network.[33] NSFNET collected three classes of network statistics, interface statistics; packet categorization; and intermodal delays.[34] However, when the backbone was

---

[31] *See* FCC Quarterly Inquiries and Complaints Reports, http://www.fcc.gov/cgb/quarter/welcome.html.
[32] *See* Merit's History: The NSFNET Backbone Project, 1987-1995. http://www.livinginternet.com/doc/merit.edu/partnership.html. *See also* Claffy, Kimberly C., Braun, Hans-Werner, and Polyzos, George C., *Tracking Long-term Growth of the NSFNET;* Available at http://cseweb.ucsd.edu/groups/csl/pubs/journal/cacm.94.ps. *For a list of metrics see* http://www.cc.gatech.edu/gvu/stats/NSF/merit.html.
[33] *See* Braun, Hans-Werner and Claffy, K. *post-NSFNET statistics collection*, 1 – 2; Available at http://www.caida.org/publications/papers/1995/pnsc/postns.pdf.
[34] *See* Claffy et al *Tracking Long-term Growth of the NSFNET.*

decommissioned in the mid-1990s to privatize the network infrastructure, integration of data collection into network equipment and access to resulting data ceased. Since that time, access to data on Internet traffic, topology, routing, and security have diminished and Internet researchers have struggled to conduct valid and reproducible scientific experiments under increasingly restrictive constraints.[35] This in turn, has substantially reduced the transparency on the Internet that was an essential component of its success and has limited collaboration and the diffusion of best practices across the Internet. Innovation in networking technology is overwhelming shaped by service providers, whose incentives are often more aligned with technological improvements that bring in additional revenues rather than more efficiently or effectively improve the performance of networks. At the same time, policymakers are almost entirely dependent upon the service providers for data on the workings of the Internet as a means to determine appropriate policies.

What is needed is a sustained effort to bring greater transparency and promote open, data collection on broadband services and the Internet in the U.S. Already, there are data collection efforts underway to improve transparency to the Internet, empower consumers, and promote research and innovation projects such as Measurement Lab[36] and BroadbandCensus.com[37]. In addition, researchers have developed proposals such as the COMMONS project to provide access to performance and traffic data on the Internet networks.[38] The FCC can build-upon these efforts and develop policies to improve and enlarge its own data collection efforts. Key to this effort will be utilizing many testing methods and measurement tools toward maximizing the openness and transparency of broadband measurements—including making data publicly available to allow for independent verification and analysis.

We encourage the Commission to think broadly about measurements and data collection, promote efforts that will empower consumers and the FCC to assess the capabilities of broadband services, and create viable sources for data on Internet traffic and network performance for researchers and policymakers. NAF proposes a comprehensive approach to measuring broadband, encompassing both passive and active measurement processes.

Physical Infrastructure Description

Figure 2 below depicts the network segments providing connectivity from an end-user to the content hosted on the public Internet represented by the numbers in yellow circles.

1. **Public Internet:** Content on the Public Internet is hosted by multiple service providers, content providers, and other entities in a geographically diverse (worldwide) manner.

2. **Internet Gateway/Border Router:** The Internet Gateway or Border Router is the closest peering point between the Internet backbone and the internal middle mile network of an Internet Service Provider (ISP) and/or Internet Exchange Points (IXP).

[35] *See The COMMONS Initiative*; Appendix 1, p. 5.
[36] http://www.measurementlab.net.
[37] http://www.broadbandcensus.com.
[38] *See The COMMONS Initiative*; Appendix 1, p. 5.

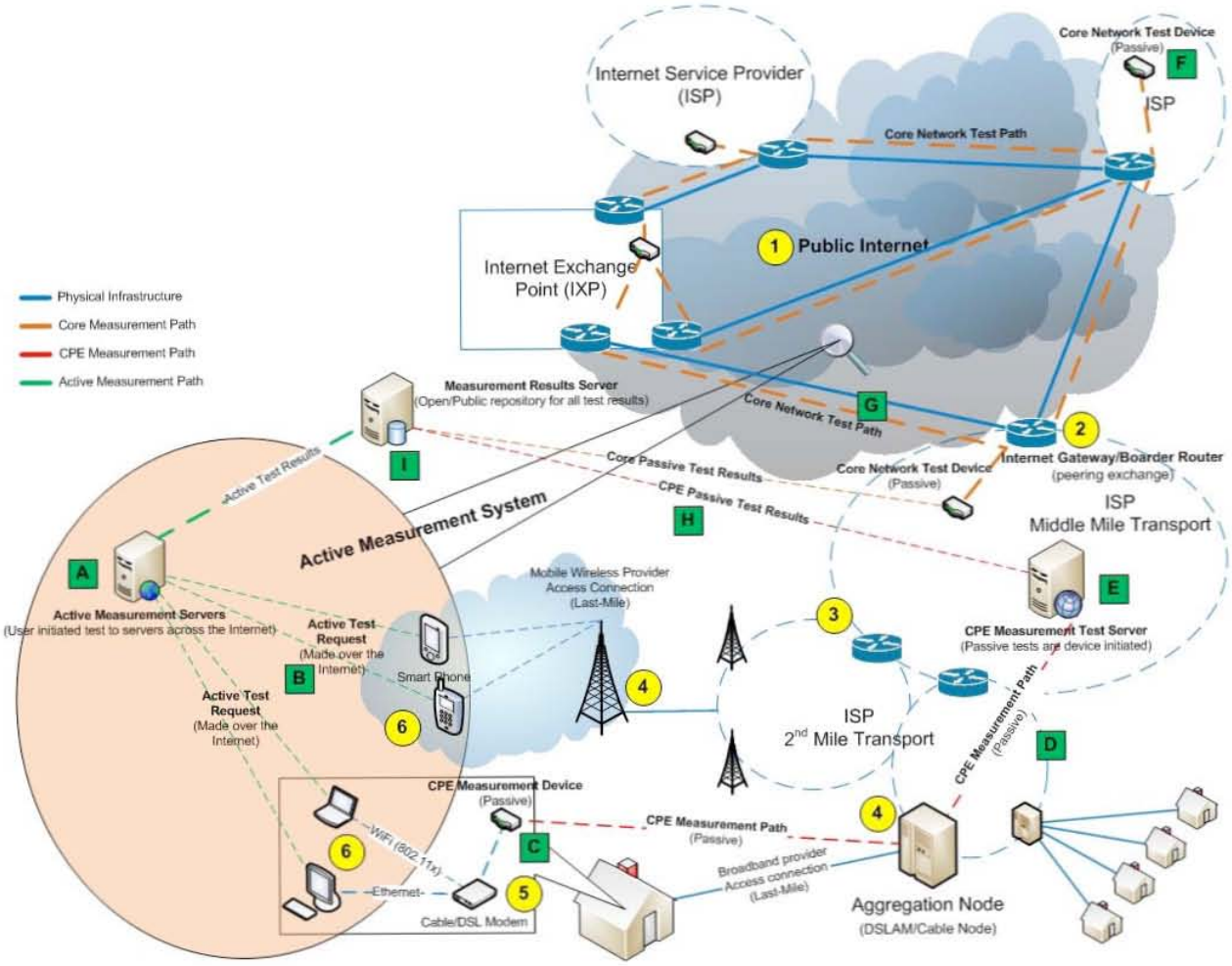
3. **Link between Middle Mile and 2nd Mile network:** The connection between the middle mile network and a 2nd mile network is often provider managed.

4. **Aggregation Node (Link between 2nd Mile and Last Mile network):** The 2nd mile network terminates at an aggregation node, such as a cable node, DSLAM, satellite, fixed cellular tower, etc., the first aggregation point from the provider's 2nd mile network to the start of the last mile network.

5. **Modem:** The Customer Premise Equipment (CPE) is the last connection point to the managed network that is often managed by the provider. Examples of a CPE include DSL modem, cable modem, satellite modem, mobile cellular device or Optical Network Terminal.

6. **Consumer Devices:** Consumer devices, such as desktop/laptop computers or cellular phones connect to the modem through an internal wired or wireless home network connection. Hardware and software used to access and process content are usually managed by the consumer.

Figure 2: Measuring Broadband Services and the Internet



Proposed Measurement System

The above figure depicts our proposed system for measuring network segments and use from the end-user and points within public Internet indicated by the letters in green squares. The numbered and lettered items below correlate with those items in the figure above.

A. **Active Measurement Servers:** Active Measurement Servers process user-initiated tests and are located within provider's Middle Mile network and at Internet Exchange Points to provide the best possible connection to Internet Gateway/Border Routers (circle 2).
B. **Active Measurement Test Request:** Users can, on computers and other consumer devices (circle 6), request a test of their network by Active Measurement Servers located within their provider's Middle Mile networks or within other provider's Middle Mile networks over the Internet.
C. **CPE Measurement Device:** Managed devices located behind Last Mile Customer Premise Equipment (CPE) that request passive (not initiated by a user) network measurements of the providers network from the CPE Measurement Server (E).
D. **CPE Measurement Path:** A CPE Measurement Test connects to a CPE Measurement Server (E) after flowing from the Modem (circle 5), through the Aggregation Node (circle 4), and the 2nd Mile network into the Middle Mile (circle 3).
E. **CPE Measurement Server:** The CPE Measurement Server is the end point of the CPE Measurement Path and where testing tools and results are initially stored. The CPE Measurement server determines which tests, and at what frequency, the CPE Measurement Device initiates requests.
F. **Core Network Test Device:** Core Network Test Devices are located within provider's Middle Mile networks and Internet Exchange Points with best available connections to Internet Gateway/Border Routers (circle 2). They take perform passive (not initiated by a user) measurements of Middle Mile to Middle Mile network states. The testing tools on Core Network Test Devices will be able to both initiate a test and respond to a request from another Core Network Test Device. Results are then relayed directly to the Measurement Results Server (I).
G. **Core Network Measurement Path:** The test path taken by Core Network Test Device's will be across primary peering points between ISP's and IXP's networks.
H. **Passive Test Results:** Results from the CPE Measurement Devices (C) and Core Network Test Devices (F) are sent to a central Measurement Results Server (I).
I. **Measurement Results Server:** All measurements from both passive [(CPE (C) and Core devices (F)] and active test (A) are stored on a Measurement Results Server, providing a central repository. All results are stored in a standard open format and available to the public for review analysis, and to researchers for independent verification of the data.

Active vs. Passive Measurement

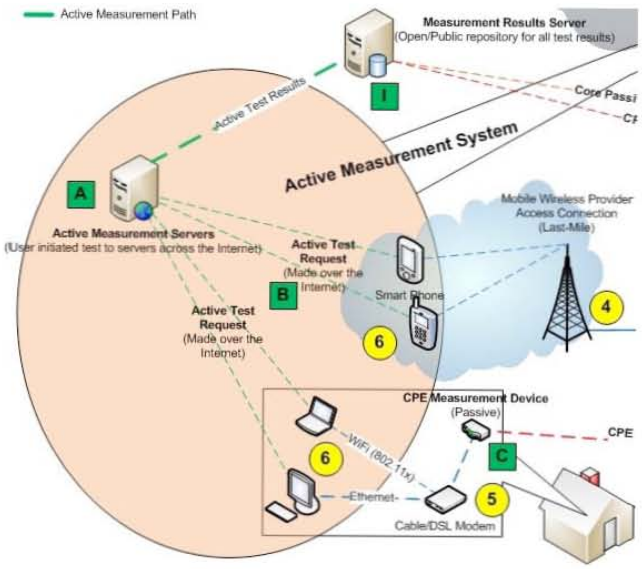
As the Commission considers methods for measuring broadband services, it is important to make a distinction between user-initiated “active” and “passive” measurements. For purposes of NAF’s proposals and the above diagram we are defining “active” measurements as those

initiated by an end-user, such as a broadband subscriber, and "passive" measurements as non-user initiated. This definition slightly differs from the research community's categorizations that recognize a passive test as one that observes the behavior of test object during normal operation and does not initiate the activity or use its own data as an input into the test; and defines an active test as one that introduces data from a transmission and analyzes the resulting network performance. While the definition of active and passive test used in this document is not identical to that often used in the research, there are many instances where tests can fit under both definitions.

Examples of active measurements include basic speedtest tools[39] to more sophisticated tools such as those found on the Measurement Lab platform.[40] Active measurements challenges include: (1) deployment to insure low impact on the infrastructure; (2) prevention of use of tools for Distributed Denial of Service attacks; (3) accountability of measurement source; (4) analysis of bias due to self-selection of sources (by volunteers); and, (5) validation of the integrity of resulting data.[41] Client-side automatically initiated passive measurement infrastructures are like those integrated into the NSFNET backbone described above. Hardware and software integrated into the networking technology or connected "boxes" collect and track traffic and performance data over a network over time. Among the key challenges of passive measurements is protecting privacy as well as ensuring the system and resulted data is not manipulated by a particular operator or application.

1. Active Measurement (End-User Initiated Tests)

Figure 3: Active Measurement System



[39] Examples include http://www.speedtest.net/, http://www.speakeasy.net/speedtest/, and http://www.dslreports.com/speedtest?flash=1.
[40] http://www.measurementlab.net/measurement-lab-tools.
[41] *See The COMMONS Initiative*; Appendix 1.

Active measurements are initiated by an end-user, such as a broadband subscriber, and measure the network during a specific task (square B). Examples include basic speedtest tests such as those provided by websites such as Speedtest.net[42] and others, but they can also include measuring more sophisticated performance and diagnostic tests to determining if an ISP is throttling or blocking specific applications.[43] The possible uses of active measurement systems include: 1) consumers testing the performance capabilities of their broadband connection; 2) diagnostic tools to determine problems with a broadband connection or why an application is not working; 3) tools for consumers and regulators to compare actual broadband performance versus advertised; and, 4) experimentation and data collection for Internet researchers and regulators.

A sample architecture of an active measurement system is provided above in Figure 3. Measurement servers process the user initiated tests and are located within provider's Middle Mile network and Internet Exchange points (square A). Ideally for most situations, servers are located as close as possible to a provider's Gateway/Border Router to accurately measure performance metrics and networking characteristics on the last-mile connection. (However, active measurement tools may also seek to examine the entire path of a transmission along multiple networks.) Broadband users then on their consumer devices such as PCs, laptops, or smartphones can run a test from the measurement server, which then processes the test, collects the data, and provides the user with results.

An example of a measurement system for consumers and researchers is Measurement Lab (M-Lab).[44] It is an open, distributed server platform for researchers to deploy Internet measurement tools. The goal of M-Lab is to advance network research and empower the public with useful information about their broadband connections.[45] M-Lab differs from a number of other active measurement efforts by providing: 1) an open platform that assists scientific research by provisioning widely-distributed servers and ample connectivity for researchers' use; 2) server-side tools that are open-sourced software that allows third-parties to develop their own client-side measurement software; and, 3) open and publicly accessible data about Internet measurements for the research community, policymakers, and the public.[46]

As the Commission considers utilizing testing and measurements to improve consumer information and transparency on broadband services and the Internet, NAF believes openness and publicly available "raw" data is key to maximizing the benefits of active measurements for consumers, researchers, policymakers, innovators, and even service providers. The extent to which active measurements can be utilized for assessing the performance of a broadband service and collecting accurate data is dependent upon the validity of the measurement tool. Users, researchers, policymakers and service providers must be able to verify the accuracy of the measurement. Open sourcing allows for all parties to truly understand the test methodology of a

---

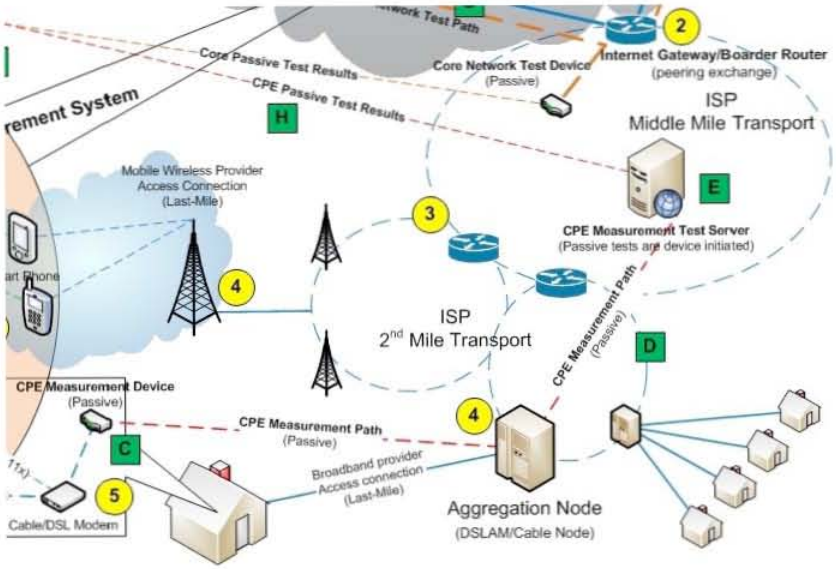
[42] *See* http://www.speedtest.net/. *See also* http://www.speakeasy.net/speedtest/ and http://www.dslreports.com/speedtest?flash=1.
[43] http://www.measurementlab.net/measurement-lab-tools
[44] Measurement Lab was founded by the NAF, the PlanetLab Consortium, Google Inc. and academic researchers. *See* http://www.measurementlab.net.
[45] *See* Appendix 5 Exhibits A and B.
[46] Data from two of M-Lab's tools is publicly available on via Amazon Web Services, allowing anyone to make use of this information without restriction, under a "no rights reserved" Creative Commons Zero waiver. *See* http://www.measurementlab.net/news/2009/dec/10/calling-all-researchers-m-lab-data-now-available-amazon-ec2

particular measurement tool and encourages continued refinement and improvement. As NAF proposed above, the FCC could allow consumers to submit active measurement results to the Commission as part of an improved consumer complaint process. Unlike closed, proprietary tools, open source tool would allow all affected parties including service providers to examine the code and assess the validity of the measurement instrument.

The usefulness of measurements of broadband connections and the Internet to improve research, innovation, and public policy is also substantially tied to open and accessible data. For many active measurement tools or services, data collected from individual tests is often unavailable to the public, researchers, or policymakers (or is available only for a fees). This substantially limits the usefulness of the data. It is critical that any data collected through an FCC-led effort, be open and publicly available to encourage robust research, analysis and independent verification.

2. Passive Measurement (Customer Panel Devices)

Figure 4: CPE Measurement System



Similar to user-initiated measurements, passive measurements could be utilized to test last-mile connections without initiation from an end-user. These measurement projects draw on the inspiration of SETI@Home to develop passive client-based measurement software and/or hardware to collect user data.[47] Users voluntarily install software or some type of CPE measurement device (square C) that passively runs tests under controlled conditions and report them back to measurement server (square E.)

[47] *See* Anderson, David P., Cobb, Jeff, Korpela, Eric, Lebotfsky, Matt, and Werthimer, Dan; *SETI@home: An Experiment in Public Resource Computing* 45 COMM. OF THE ACM 56, 56 (2002) (explaining that Search for Extraterrestrial Intelligence at Home (SETI@Home) is a project in which "[m]illions of computer owners worldwide contribute computer time to the search for extraterrestrial intelligence, performing the largest computation ever.").

An example of this is SamKnows "Sandbox," a configured monitoring devices in homes across the UK running tests and collecting performance data 24 hours a day, 7 days a week, 365 days a year.[48] The benefits of this approach are that measurements can be collected in a consistent manner, over time and as a representative sample. In 2008, OFCOM, the United Kingdom's telecommunications regulator, partnered with SamKnows to carry out a comprehensive study of broadband provider performance.[49] OFCOMselected SamKnows as its technical partner in the project, and SamKnows provided the in-home hardware devices, methodology and funding the deployment. OFCOM then commissioned a market research firm to recruit and manage a representative panel of UK broadband users.[50]

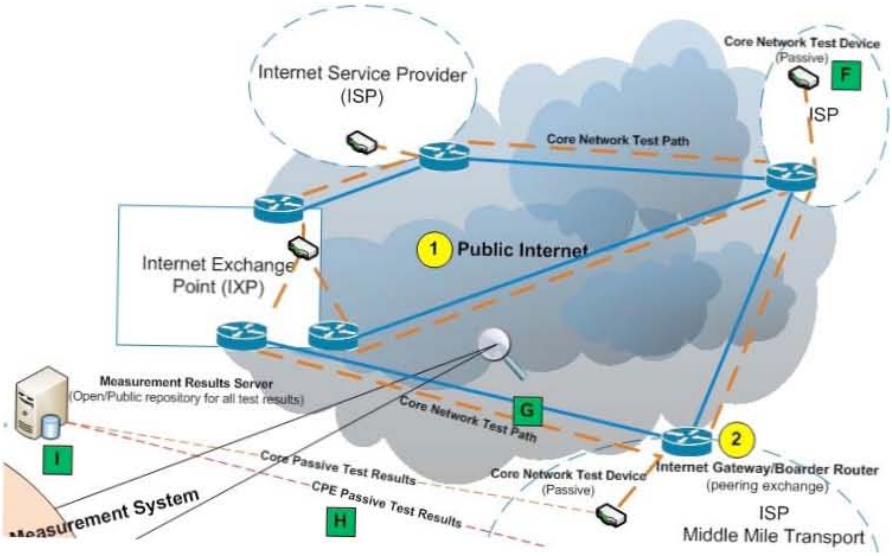
NAF believes a similar approach would be beneficial to FCC data collection and provide policymakers important data for assessing and monitoring the state of broadband and the Internet in the U.S. Such an effort should include a representative panel of U.S. broadband users that includes under-represented populations, and subscribers from as many broadband providers as possible. Beyond a single report, the FCC could consider utilizing this panel approach to consistently measure broadband. Results from the panel would be a useful addendum to the Commission's annual report on the availability of high-speed and advanced telecommunications services.[51] If the Commission considers utilizing representative panels, it is once again essential that it focus on maximizing openness and transparency in the measurement tools and processes and make these data publicly available to allow for independent verification and robust research and analysis.

---

[48] *See* Samknows Sandbox at http://www.samknows.com/broadband/samknows-labs.php?page=samknows-labs-samknows-sandbox.
[49] *See* Ofcom Benchmark at http://www.samknows.com/broadband/performance.php?page=performance-ofcom-and-samknows.
[50] *Id.*
[51] *See Inquiry Concerning the Deployment of Advanced Telecommunications Capabilities to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Acto of 1996: Fifth Report*; GN Docket No. 09-45, FCC 08-88 (rel June 12, 2008).

3. **Passive Middle-Mile and Backbone Measurement**

Figure 5: Core Network Measurement System



Since the privatization of the NSFNET backbone, researchers and policymakers have limited access to fundamental performance and traffic data on the middle-mile and backbone portions of the Internet. As the Commission examines complex issues of network congestion and network management, it is entirely dependent on analysis of traffic and usage data from service providers. Data that is publicly accessible, and independently verifiable would support independent analysis of actual Internet traffic, and inform salient debates on technical, economic, policy, privacy, and social issues relating to the Internet.

Among the areas of greatest need is access to fundamental performance and traffic data from peering and IXPs. The above detail from Figure 2 illustrates a system of passive devices (square F) placed immediately within provider's and Internet exchange point's networks as close to the Internet Gateway/Border routers (circle 2) as possible. These devices would be taking both passive and active tests from core paths between ISP's and IXP's (square G). As an optical fabric, the measurement devices could support direct measurement of wavelengths or provide SNMP counters as supported in the attached equipment.[52] Results from all tests could be stored and available to the public for review, analysis, and verification on a results server (square I).

Most ISPs, middle-mile, and backbone providers already collect information on traffic flows and volume.[53] However, there is limited, if any, public disclosure of the raw traffic data. Reports and analysis are entirely conducted or directed by the provider. Policymaking and innovation, would substantially benefit from requirements for these providers to disclose fundamental information Organizations such as the Cooperative Association for Internet Data Analysis (CAIDA) have attempted to fill this void, through placing passive monitoring equipment at several different data types at geographically and topologically diverse

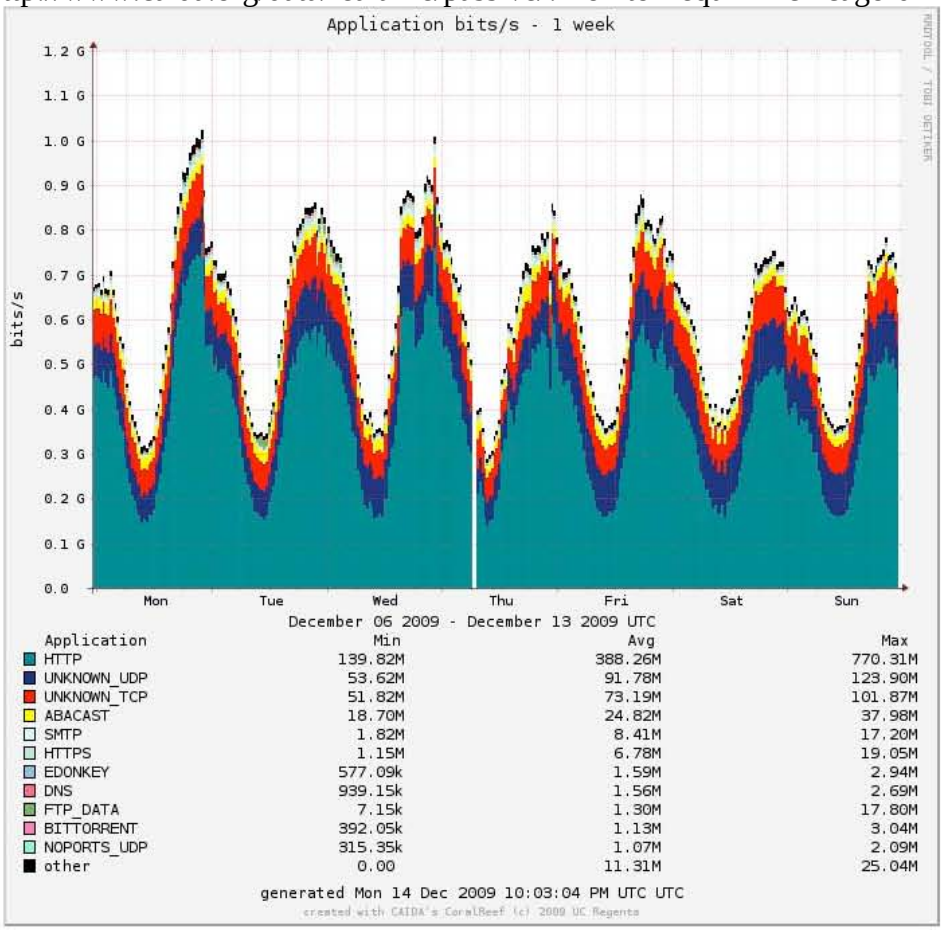
[52] *See The COMMONS Initiative*; Appendix 1.

[53] *See for example* "Integrated Routing and Traffic Analysis and Modeling for Internet Peering," Packet Design, Technical Brief, http://www.fvc.com/FVC/fvcweb/Files/IntegratedIPRoutingAndTrafficAnalysis.pdf.

locations, and makes this data available to the research community to the extent possible while preserving the privacy of individuals and organizations who donate data or network access.[54] But, the number of sites is inherently limited as research organizations such as CAIDA do not have access to the vast majority of peering reports.

Researchers, competing providers, and consumers alike benefit from more transparency in the core of the Internet. Along with tests that determine network connection states (e.g. capacity, congestion, latency, jitter, throughput, prioritization), tests that identify use trends should be conducted. Researchers at CAIDA have implemented both and active and passive monitoring system allowing the public to view near real-time graphs of network usage trends (Figure 6). Policymakers, researchers, ISPs, network device makers, and customers alike need independent analysis of the health of the Internet pathways and the ability to go as deep as needed into the data to promote a thriving future Internet.

Figure 6: CAIDA Chicago Passive Monitor
(http://www.caida.org/data/realtime/passive/?monitor=equinix-chicago-dirA)



Such an effort should further encourage greater access for academic and research organizations to access a greater number of IXPs for passive monitoring and a collection of measurements that provide an indication of overall backbone health (e.g., capacity, congestion,

[54] http://www.caida.org/data/passive/.

actual use, and throughput) and utilization trends. This effort would provide more information from the inside rather than the basic information available from outside such as Keynote's Internet Health Report[57] or AnalogX's Internet Traffic Report[58] both of which are limited to round-trip travel time using the ping utility.

IV. CONCLUSION

The current rules to ensure consumers' access to relevant information about the communication services they are purchasing are grossly insufficient. Service providers overpromise on the capabilities of their service and routinely fail to disclose limitations to services and hidden fees – leading to consumer confusion and frustration. Substantial changes to the Commission's existing rules are necessary to remedy these problems. Commission rules should require providers to disclose vital information on the performance capabilities, price, and terms of the service offering before consumers purchase a service. Similarly, existing customers should receive advanced and explicit notification on any changes to the technical capabilities, terms of service or use, privacy policy, network, management practices, and any other changes to the service.

In addition, policymakers, researchers, and innovators have access to little information about the workings of the Internet. What is needed is a sustained effort to bring greater transparency regarding broadband services and the Internet in the U.S. The FCC can build upon these efforts and develop policies to improve and enlarge its own data collection efforts. Key to this effort will be utilizing many testing methods and measurement tools to maximize the openness and transparency of broadband measurements and ensure that data is publicly available and to allow for independent verification and robust analysis. Taken together, these efforts will bring much-needed transparency to the broadband marketplace, empower consumers, spur research and innovation, and improve public policy.

Respectfully submitted,
/s/

Benjamin Lennett
James Losey
Dan Meredith
Robb Topolski
Sascha Meinrath

Open Technology Initiative
New America Foundation
1899 L Street, NW
Suite 400
Washington, DC 20036
oti@newamerica.net

December 14, 2009

[57] http://www.internetpulse.net/.
[58] http://www.internettrafficreport.com/.

Appendix 1

THE COMMONS INITIATIVE: COOPERATIVE MEASUREMENT AND MODELING OF OPEN NETWORKED SYSTEMS*

Sascha D. Meinrath† and kc claffy‡

I. INTRODUCTION

Over the past several years, interest in municipal wireless and community networking has increased dramatically.[1] Thus far, these initiatives have generally focused on networking local communities. The next evolution in networking involves peering these networks together.[2] Research on broadband service provision is desperately needed to help forge new national telecommunications policies and inspire innovation in networking technologies.[3]

With this goal in mind, the Cooperative Association for Internet Data Analysis ("CAIDA") held a workshop to discuss—and ultimately propose—collaboration among researchers and networks to simultaneously solve three

---

* The COMMONS Strategy Workshop brought together leaders from across North America to discuss issues related to broadband service provision and to strategize about how to interconnect existing networks to one another utilizing national fiber assets. An earlier version of this article was published on the CAIDA Web site. The authors wish to thank all the participants in the COMMONS project.

† Sascha D. Meinrath is Research Director of the Wireless Future Program at the New America Foundation.

‡ kc claffy is the principal investigator for the Cooperative Association for Internet Data Analysis ("CAIDA") and Resident Research Scientist based at the San Diego Supercomputer Center.

1 *See* MUNIWIRELESS.COM, STATE OF THE MARKET REPORT (2006) (on file with author).

2 Peering is "a relationship established between two or more ISPs (Internet Service Providers) for the purpose of exchanging traffic directly, rather than doing so through a backbone Internet provider." NEWTON'S TELECOM DICTIONARY 705–06 (23d ed. 2007).

3 Press Release, Rep. Edward J. Markey, Markey Addresses Consumer Federation of America on Broadband and Internet Policy (Feb. 1, 2007), http://markey.house.gov/index.php?option=com_content&task=view&id=2577&Itemid=141.

acute and growing problems facing the Internet. First, there exists a self-reported financial crisis in the Internet infrastructure provider industry that poses a threat to broadband growth and American competitiveness. Second, a data acquisition crisis has stunted the field of network science. Finally, emerging community, municipal, regional, and state networks need additional broadband connectivity but face limited provider, service level, and usage options.

The Cooperative Measurement and Modeling of Open Networked Systems ("COMMONS") Initiative proposes to build or partner with a collaborative national backbone to connect participating community, municipal, regional, and state networks to one another and to the global Internet. The COMMONS provides a platform for Internet researchers to study this infrastructure. It also provides a low-cost medium for networks to peer with one another. This approach will provide vital research results for policymakers across the country and around the world.

Part II of this article describes the findings from the initial COMMONS Strategy Workshop held in December 2006. Part III outlines relevant open research problems identified by the participants. Part IV proposes a framework for the end-to-end interconnection of networks at all levels on a national scale. Finally, the article concludes with a discussion of the steps necessary to bring about such a networking arrangement. Further, this section highlights the potential benefits to the scientific community, network operators and developers, key decision makers, and the general public.

II. THE COMMONS STRATEGY WORKSHOP

A. Purpose

On December 12–13, 2006, CAIDA hosted the first COMMONS Strategy Workshop at the San Diego Supercomputer Center on the Campus of the University of California at San Diego.[4] Workshop participants included a collection of relevant individuals and entities, such as community and municipal wireless builders, measurement experts, wireless technologists and researchers, policymakers, legal and privacy experts, and industry participants.[5] Workshop attendees discussed the design, creation, and operation of an experimental infrastructure that could simultaneously address three core crises: (1) the gap between those who benefit from digital technology and those who do not, commonly known as the digital divide; (2) the scientific integrity of network re-

---

[4] *See* CAIDA, COMMONS Workshop Agenda, http://www.caida.org/workshops/commons/0612/agenda.xml (last visited Apr. 4, 2008).

[5] *See* CAIDA, COMMONS Workshop Participants List, www.caida.org/workshops/commons/0612/list.xml (last visited Apr. 4, 2008).

search; and (3) the inability to empirically inform policy decisions at a critical juncture in telecommunications history.

The United States is facing a worsening broadband crisis. Over the past half-decade, the United States has fallen behind a growing list of industrialized nations in delivery speeds, price per megabit, broadband penetration rates, and other facets of broadband service provision.[6] Rural and poor communities face additional obstacles, often receiving little or no broadband access or being forced to pay higher service rates when they do have access.[7] Due to regulatory, political, and market constraints of incumbent local exchange carriers and other broadband providers, Internet researchers have been unable to study mission-critical aspects of the Internet[8] and the state of its current robustness, capacity, usage, and problem areas. Therefore, potential solutions to these issues continue to be conjecture, rather than empirically-backed analysis.[9] Meanwhile, telecommunications regulators and policymakers have increasingly called for a methodologically sound study of Internet usage, analysis of potential failure points, and improvements to this vital infrastructure.[10]

The COMMONS provides an opportunity to address these shortcomings within a single national framework. By creating a national peering infrastructure that interested network operators may choose to join, the COMMONS will provide numerous opportunities and benefits for a range of different constituencies including: low-cost transport; the ability to buy bandwidth in bulk and share the cost-savings among the COMMONS partner organizations; and empirically grounded analyses of traffic flow, congestion points, and underutilized links.

---

[6] S. DEREK TURNER, FREE PRESS, BROADBAND REALITY CHECK II: THE TRUTH BEHIND AMERICA'S DIGITAL DECLINE 3–4 (2006), *available at* http://www.freepress.net/files/broadband_report.pdf.

[7] U.S. GOV'T ACCOUNTABILITY OFFICE, TELECOMMUNICATIONS, BROADBAND DEPLOYMENT IS EXTENSIVE THROUGHOUT THE UNITED STATES, BUT IT IS DIFFICULT TO ASSESS THE EXTENT OF DEPLOYMENT GAPS IN RURAL AREAS 4 (2006), http://gao.gov/new.items/d06426.pdf.

[8] COMM. ON NETWORK SCIENCE FOR FUTURE ARMY APPLICATIONS, NAT'L RESEARCH COUNCIL, NETWORK SCIENCE 7 (2005).

[9] *See* NAT'L SCI. & TECH. COUNCIL, FEDERAL PLAN FOR CYBER SECURITY AND INFORMATION ASSURANCE RESEARCH AND DEVELOPMENT (2006), *available at* http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf (exemplifying the interagency framework that is needed to provide an adequate level of cyber security and information assurance capabilities and technologies).

[10] *See* Bob Wallace, *NTCA: FCC Commissioner Calls for Sweeping Regulatory Reform: Candor from Copps Counts with Rural Telco Crowd*, TELECOMM. ONLINE, Feb. 7, 2006, http://www.telecommagazine.com/newsglobe/article.asp?HH_ID=AR_1706 (explaining that the United States lacks a national broadband strategy that effectively reaches rural America); *see also* Press Release, Rep. Edward J. Markey, *supra* note 3 (noting that the United States has low broadband subscribership within the global market).

Peering will be conditionally available to local, state, and federal government entities, academic institutions, community Internet initiatives, and commercial entities based upon three conditions. First, networks will make select operational data available to the COMMONS researchers under appropriate legal data sharing and privacy guards. Second, the attached networks must agree to develop and abide by the COMMONS's policies, which will be based upon research results of empirical data analyses of network usage. Third, participating networks must abide by the Acceptable Use Policies[11] created by the COMMONS Coordination Committee.[12] The COMMONS will impact both the Internet industry and policymaking broadly, by providing substantial real-world data on Internet traffic at the national level and informing analyses, regulatory discussion, and technological innovation. It also promises to raise the intellectual merit of the entire field of Internet science through increasing standards of data collection and sharing within the research community.

The telecommunications sector has not yet recovered from the privatization and commercialization of Internet infrastructure, which began in the early 1990s. After a decade of boom and bust, consolidation continues, though the number of Internet service providers left to consolidate has greatly diminished.[13] Furthermore, the largest of the remaining providers have publicly insisted that they will not be able to make the required investment to build-out broadband infrastructure without more flexible pricing strategies to recover costs.[14]

---

[11] CAIDA uses the following Acceptable Use Policies to govern its data collection activities: (1) passive monitors will run only strictly necessary services and will be kept up-to-date with necessary security patches and operating system upgrades to limit security risk; (2) only a minimal number of CAIDA personnel trained in protecting user privacy and secure handling of data will have accounts on passive data monitors; (3) no packet payloads will be permanently recorded without specific permission from the hosting site; (4) traces will not be released from CAIDA custody unless the IP addresses are anonymized using prefix-preserving anonymization (or other current state-of-the-art anonymization technology). CAIDA personnel and collaborators who are physically present in CAIDA offices may have access to non-anonymized packet headers for research purposes; (5) CAIDA will require registration from users who wish to download anonymized traces; and (6) traces will be distributed internationally to registered users, although we are bound by the Department of State's International Traffic in Arms Regulations. *See* COMMONS Site Acceptable Use Agreement, http://www.caida.org/projects/commons/aup/ (last visited Apr. 19, 2008).

[12] The COMMONS Coordinating Committee will consist of representatives from active partners on the COMMONS Project and will help oversee the COMMONS Project, provide feedback on the COMMONS documents, and help with outreach.

[13] *See, e.g.*, Tom Spring, *ISPs Share Urge to Merge*, CNN, Mar. 2, 1999, http://www.cnn.com/TECH/computing/9903/02/ispmerge.ldg/index.html (describing the rapid consolidation of Internet Service Providers during the late 1990s).

[14] Marguerite Reardon, *AT&T Chief, FCC Chair Clarify on Net Neutrality*, CNET-NEWS, Mar. 21, 2006, http://www.news.com/AT38T-chief%2C-FCC-chair-clarify-on-New-neutrality/2100-1034_3-6052239.html.

By removing from commercial providers the responsibility for supporting Internet service delivery to unprofitable areas, the COMMONS will measurably alleviate the economic pressure on these providers. Additionally, the COMMONS offers an unprecedented opportunity to establish standards of scientific integrity in the field of Internet research by providing rigorous empirical data against which to validate theory, modeling, and simulation activities. Furthermore, because the COMMONS will support public analysis of actual Internet traffic, it will inform debates on increasingly important technical, economic, policy, privacy, and social issues relating to the Internet. Finally, the COMMONS not only allows struggling community networks to cost-share a financially daunting component of their connectivity, but it also provides a forum for the cooperating networks and the research community to share lessons with one another.

B. Background

The first general purpose Internet backbone,[15] NSFNET, was funded and administered by the National Science Foundation to support the networking needs of the research and education community.[16] It was implemented to provide continuously collected data on the function and usage of the network.[17] When this backbone was decommissioned in the mid-1990s as a part of the government's strategy to privatize the network infrastructure, the attached academic networks transitioned to self-sustaining funding models.[18] Unfortunately, since that time, access to representative data on Internet traffic, topology, routing, and security has diminished as Internet researchers have struggled to conduct legitimate, reproducible scientific experiments under increasingly restrictive constraints. Furthermore, many of the measurements and lessons learned by commercial Internet providers over the last decade were not retained, or if retained, not shared for fear of providing an advantage to marketplace competitors.

Obstacles to the collection and analysis of traffic data on the commercial Internet pose not only formidable technical and engineering challenges, but also include more daunting legal, logistical, and proprietary considerations. Data acquisition is further complicated by the upgrades to new networking

---

[15] The backbone of a network is "the part of the communications network which carries the heaviest traffic. The backbone is also that part of a network which joins LANs together – either inside a building or across a city or the country." NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 146.

[16] NAT'L. SCI. FOUND., THE INTERNET: CHANGING THE WAY WE COMMUNICATE 6 (2008).

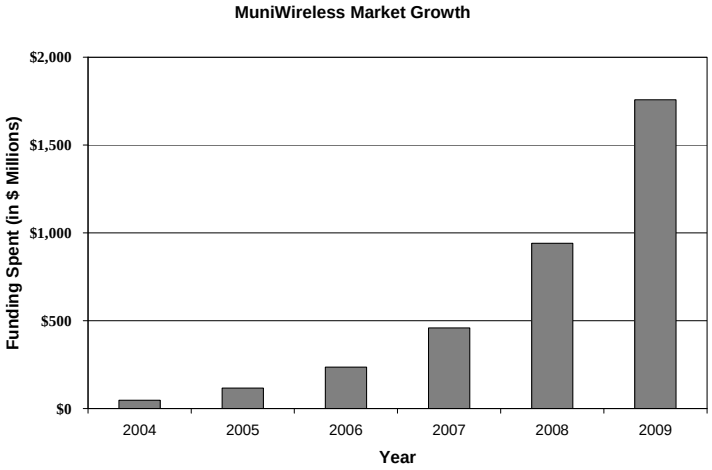
[17] *Id.* at 11.

[18] *Id.* at 12.

technologies that are generally prohibitively expensive or difficult for researchers to monitor. Diverting resources to statistics collection takes those resources directly away from forwarding of packets, which tends to drive commercial providers toward switching from vendors that sacrifice potential research functionality in exchange for performance. As a result, core backbone routers often do not have the functionality to gather the intricate data needed to support scientifically sound modeling, simulation, and analysis efforts.[19] In combination, these issues leave the Internet research community continually struggling to validate research theory. And yet, as the world becomes increasingly dependent on the Internet infrastructure, it becomes ever more critical to understand not only Internet structure, workload, and dynamics, but also the economic forces that constrain their evolution.

The Internet is at a unique turning point in its history—a time when wireless infrastructure that is "too inexpensive not to deploy" is starting to gain traction in community and public settings. Indeed, in the last several years, the growth of wireless access has increased dramatically. According to MuniWireless.com, in the municipal wireless market alone, the sector has grown from $47.4 million in 2004 to $235.5 million in 2006, with the market predicted to exceed $1 billion before the end of the decade.[20]

Figure 1. Growth of the Municipal Wireless Market (2004–2009).[21]



[19] kc claffy & Tracie Monk, *What's Next for Internet Data Analysis? Status and Challenges Facing the Community*, 85 PROCEEDINGS OF THE IEEE 1563–71 (1997).

[20] MUNIWIRELESS.COM, *supra* note 1, at 8.

[21] *Id.*

Looking at the United States, one can see both that the diversity of networks is substantial and that their numbers are rapidly increasing.

Table 1. Number and Type of Municipal Wireless Networks—July 2005 to December 2006[22]

Type of Network	July 2005	Feb. 2006	April 2006	June 2006	Sept. 2006
Region/Citywide	38	56	58	59	68
City Hot Zones	22	29	32	32	43
Municipal or Public Safety Use Only	28	32	35	35	35
Planned Deployments	34	59	69	121	135

Although the growth in municipal wireless networks may look promising, the United States is falling behind other countries with regard to Internet infrastructure penetration.[23] However, the extent to which it is lagging has been obfuscated by faulty and opaque measurement and analysis methodologies.[24] In his seminal analysis and report on the state of American broadband, S. Derek Turner, Free Press Research Director, states that policymakers must:

> [R]equire the FCC to improve its data collection on broadband markets. Policymakers cannot adequately assess the problems in the broadband market, nor identify the most appropriate solutions, if the FCC provides poor information. The starting point should be a more precise measure of which geographic areas have service (using a smaller unit than the ZIP code). Beyond that, carriers should be required to report the percentages of households where broadband service is available in every service area, the percentage of households that subscribe, and the average cost per megabit of throughput. This evidentiary record will allow an accurate analysis of the problems we face and foster solutions that will achieve results.[25]

As an example of policymakers' failures, until recently the Federal Communications Commission ("FCC") defined broadband as "data transmission speeds

---

[22] *Id.* at 29.

[23] *See* Rob Kelley, *Broadband Lag Could Hurt the U.S.*, CNNMONEY, June 17, 2005, http://money.cnn.com/2005/06/16/technology/broadband/index.htm.

[24] *See* TURNER, *supra* note 6, at 2, 4 ("The FCC uses misleading and meaningless measures of broadband coverage and competition."); *see also* Robert M. McDowell, Comm'r, FCC, Luncheon Address at the Broadband Policy Summit III (June 7, 2007), *available at* http://www.netcompetition.org/BB_Policy_Summit.pdf (explaining that the often-cited OECD broadband statistics are faulty in five respects, including measuring penetration per capita as opposed to per household, and geographic size and topology of the different countries in the study).

[25] *See* TURNER, *supra* note 6, at 36–37.

exceeding 200 kilobits per second (kbps), or 200,000 bits per second, in at least one direction . . . ."[26] On March 19, 2008, the FCC announced that they would raise the speed for basic broadband to 768 kbps.[27] Furthermore, the FCC has no national broadband plan. The closest thing the United States has to a national policy is a statement by George Bush calling for "universal, affordable" broadband access to all consumers by 2007.[28] In contrast, Japan has an active national initiative to bring 10 Gbps lines to all houses by 2010.[29] Note that current prices per megabit in Japan are around 30–50 cents, an order of magnitude lower than many places in the United States.[30] National broadband strategies have proven useful to the countries that have pulled ahead of the United States in terms of broadband penetration rates and price per megabit by helping structure and prioritize deployment of broadband infrastructure.

The COMMONS aims to improve the availability and reliability of Internet research by providing accurate empirical data on which Internet policy decisions can then be based. Peering networks such as the COMMONS envisions reduce the costs of research while benefiting researchers, policymakers, and the public at large.

III. QUESTIONS ADDRESSED BY THE COMMONS STRATEGY WORKSHOP

As a scientific and public-service hybrid, the COMMONS is a multi-faceted research and development endeavor that will allow measurable progress in those areas identified by participants and others. The COMMONS Strategy Workshop addressed seven key areas identified by workshop participants as critical to the initiative: (1) infrastructure issues; (2) regulatory harmonization and reform; (3) outreach and education; (4) research and technological development; (5) business model innovation; (6) expansion of broadband services; and (7) vision for the future. For participating networks, the incentive to join

---

[26] FCC CONSUMER FACTS: BROADBAND OR HIGH-SPEED INTERNET ACCESS 1 (2008), http://www.fcc.gov/cgb/consumerfacts/highspeedinternet.pdf.

[27] *See* Press Release, FCC, FCC Expands, Improves Broadband Data Collection (Mar. 19, 2008), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-280909A1.pdf

[28] *See* President George W. Bush, Remarks by the President in a Conversation on Homeownership (Mar. 26, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/03/print/200040326-15.html.

[29] Corporation for Education Network Initiatives in California, *Technology*, FIRST MILE, Nov. 12, 2004, at 2.

[30] *See* ORG. FOR ECON. CO-OPERATION & DEV., OECD COMMUNICATIONS OUTLOOK 2007, at 222–23 (2007), *available at* http://213.253.134.43/oecd/pdfs/browseit/9307021E.pdf (noting prices as low as $.22 per Mbits in Japan versus $3.18 in the United States for October 2006).

the COMMONS is similar to that of participants of Internet2,[31] National LambdaRail,[32] Quilt,[33] and thirty-three state networks trying to execute similar agendas on a smaller scale.[34] Those incentives include collective buying power, ongoing access to extensive research data, affordable fiber infrastructure, and transparent and accountable collaboration.

A. Infrastructure Issues, Expansion of Broadband Services, and Business Model Innovation

As envisioned, the COMMONS will build neutral, open optical networks by peering on National LambdaRail, Internet2, or other allied networks. Such a goal necessitates understanding local and regional demands and identifying linkages among communities seeking unfettered connectivity. Creating an efficient buy-in process for regional networks to cooperate with one another avoids duplicating the efforts of individual networks.

Peering networks, as the COMMONS envisions, will expand service to low-income constituencies, as well as those with disabilities and those that are underserved. The project will reach out to community wireless networks as well as interconnecting with Canada and international networks.

With regard to innovative business models, the COMMONS will allow assessment of the financial sustainability and scalability[35] of aggregating broadband demand. It will foster lowered bandwidth pricing through transparent empirical analysis of backhaul[36] and backbone[37] structures, and will provide the ability to evaluate the economics and performance of "quality of service" against over-provisioning to meet user and application demands.

---

[31] *See* About Internet2, http://www.internet2.edu/about (last visited Apr. 4, 2008).

[32] *See* About National LambdaRail, http://www.nlr.net/about (last visited Apr. 19, 2008).

[33] *See* Quilt, Mission, http://www.thequilt.net (last visited Apr. 4, 2008).

[34] For example, the Illinois Century Network serves over 8,000 clients throughout the state, including libraries, schools, and municipalities. Ill. Dep't of Cent. Mgmt., Next Century Network, http://www.illinois.net/next (last visited Apr. 18, 2008).

[35] Scalability refers to the size to which something can grow relatively easily. NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 812.

[36] A communications channel is backhauling when it takes traffic beyond its destination and back. In fiber networks, backhauling is a traffic management technique used to reduce the expense of multiplexing/demultiplexing. *Id.* at 145.

[37] *See supra* note 15.

B. Regulatory Harmonization and Reform, Outreach and Education, and Research and Technical Development

In addition to increasing connectivity and encouraging new business model innovation by improving accountability and research methodologies of both carriers and regulators, the COMMONS would provide empirical research to support national telecommunications policy. Such research would facilitate transparent negotiation among public and corporate interests for assets such as rights-of-way.[38]

In addition to educating policymakers and informing telecommunications policy, the COMMONS would aim to educate regulators and the public, correcting misinformation and myths using the best available empirical Internet data. These efforts would include answering concerns of users and organizations regarding online privacy. Furthermore, the data derived from the COMMONS would be provided to expert agencies for independent research and analysis.

Analysis of the COMMONS data will foster a better understanding of why networks become overloaded, including analyzing provisioning models in economic terms as well as technological terms. Furthermore, the COMMONS will provide data that facilitate the objective assessment of the social impact of proposed initiatives and will also pioneer acceptable use policies and research methodologies that balance privacy concerns against data-retention concerns.

C. Envisioning the Future

The potential impact of the COMMONS cannot be overestimated. It will directly benefit multiple constituencies across all levels of society, including private citizens, municipalities, businesses, corporations, network operators, content and service providers, public services, and the scientific community. It will also enable local and national politicians, regulators, and legislators to intelligently influence broadband policy. Future goals of the COMMONS involve developing a long-term vision for project assessment and follow-ups, building partnerships among and between academics and communities to support Internet science, and achieving universal affordable broadband access within the next ten years. Taken together, participants in the COMMONS envision a collaborative community research environment that truly will expand broadband research, access, and policy into the future.

---

[38] "Carriers and service providers . . . must obtain right-of-way to dig trenches or plant poles for cable systems, and to place wireless antennas." NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 704.

IV. PROPOSED EXPERIMENT

As discussed at the COMMONS Strategy Workshop, this article proposes that Cisco,[39] CAIDA,[40] and a national backbone resource (to be determined) join together with community, local, municipal, regional, and state networks to support a large-scale, incentive-based experiment in end-to-end network workload, performance, economic, and behavioral measurement on an unprecedented national, inter-segment, inter-provider scale. Specifically, this article proposes to develop a requirements document and roadmap to support the use of a national OC-192[41] transit backbone[42] for community wireless networks and other public sector networks to reach each other. The project will include support for native multicasting[43] of public sector services (national, state, local), including classes for any schools interested in sharing them.

In exchange for free or low-cost transit, the attached networks would agree to collaborate with network researchers in specific ways. For example, the attached networks would allow researchers access to both historical and current operational data, in appropriately anonymous form to protect the users, to study the network. Networks would agree to permit or participate in occasional openly-reviewed experiments required to test new technologies, and would make customized end-user polling tools available to community network users who individually volunteer to participate in project-related behavioral research. A prerequisite to attachment would be a commitment to adherence to responsible general administrative guidelines as set by the Policy Board to ensure that project-funded resources are used in a secure and appropriate manner.

Participating network operators would be selected to provide a broad sample of access media, connection methods, and operational environments. Participation would be conditioned on willingness to facilitate and contribute to data collection under normal operating conditions and to collaborate in occasional network-based experiments.

---

[39] Cisco Systems, Inc. is a supplier of networking equipment and network management for the Internet. Cisco Home Page, http://www.cisco.com (last visited Apr. 19, 2008). The COMMONS Strategy Workshop included two representatives from Cisco. CAIDA, COMMONS Workshop Participants List, *supra* note 5.

[40] CAIDA, the Cooperative Association for Internet Data Analysis, provides tools and analyses promoting the engineering and maintenance of a robust, scalable global Internet infrastructure. CAIDA, Home Page, http://www.caida.org (last visited April 16, 2008). The COMMONS Strategy Workshop was hosted at CAIDA's offices at the San Diego Supercomputing Center.

[41] NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 665–66.

[42] Transit backbones interconnect different networks, providing the "connective tissue" that facilitates peering and transport of data throughout the Internet.

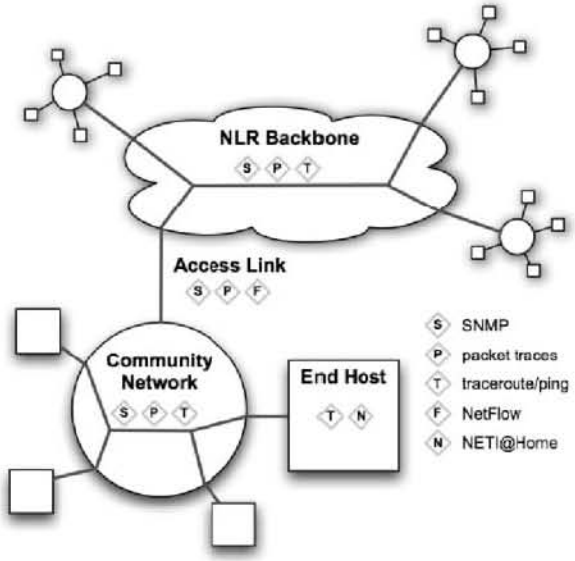
[43] Multicasting is a process whereby a data packet is sent to several different recipients (i.e., any device with a multicast address) instead of to a single machine. Unlike "broadcast" data packets, multicasting may go to many, but not necessarily all, devices within a network.

A. Possible COMMONS Measurement Architecture

Maintaining funding for Internet measurement infrastructure past the span of a given funded research project has thus far eluded the Internet research community. This failure has a substantial negative impact, not only on the goal of conducting scientifically sound Internet research, but also on all large-scale networking research that requires empirical validation. The COMMONS can directly address this crisis in a way no other existing network can. This article proposes the development and deployment of measurement infrastructure for the COMMONS that guarantees measurable progress toward restoring the intellectual strength of a wide range of Internet modeling, simulation, analysis, and theoretical research activities currently occurring without any validation. The measurement data gathered from this infrastructure will advance at least four areas: (1) support for validation of scientific research; (2) development of new measurement technology; (3) evaluation of proposed future Internet architectures; and (4) empirical answers to questions of critical national security and public policy importance.

Based on information collected during the COMMONS Strategy Workshop, this article proposes four distinct levels of measurement to support various policy and economic constraints as well as various research needs. This diversity of measurement types will facilitate correlational studies that were not previously possible. Figure 3 illustrates these four levels: (1) the backbone; (2) the backbone access link; (3) the attached community network; and (4) the end host. Figure 3 also lists examples of the types of measurements that the COMMONS should support at each specific level. Workshop participants recognize that measurements at each level will have various costs, precision, and utility. Indeed, an important early objective of the project will be to determine what data can be gathered, and at what granularity, to meet the needs of as much of the Internet research community as possible at the lowest overall cost.

Figure 2: Four Measurement Levels Incorporated into the COMMONS



1. Backbone Measurements

The COMMONS backbone will support measurements that provide an indication of overall backbone health and utilization (e.g., capacity, congestion, actual use, and throughput). As an optical fabric, the backbone could support direct measurement of wavelengths,[44] or provide SNMP[45] counters as supported in the attached equipment. The COMMONS initially proposed to collect a simple set of measurements. In the future, the COMMONS may want to invest additional development resources in optical network measurement hardware,[46] and will need to establish vetting procedures and clear disclosure procedures for adding any operational measurement functionality to the backbone.

[44] *See, e.g.*, Jörg B. Micheel, *LambdaMON – A Passive Monitoring Facility for DWDM Optical Networks*, *in* PASSIVE AND ACTIVE NETWORK MEASUREMENT 228 (Constantinos Dovrolis ed., 2005) (explaining that the lambdaMON system uses dense wavelength division multiplexing to passively monitor high performance optical networks).

[45] Simple Network Management Protocol ("SNMP") is the most common method by which network management applications can query a management agency using a supported Management Information Base. NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 852.

[46] Optical network measurement hardware is specifically designed to collect data on

2. Access Link Measurements

Access links connect the peering router of the attached community network with the peering routers of the backbone. Examples of measurements on access links include: (1) passive measurement of packet traces[47] on attached links; (2) flow measurement; and (3) SNMP counters. A more holistic analysis of network functionality can only be garnered through a multi-level, multi-method approach to network data collection. By combining passive and active measurements, focusing on data collection on different links of a network, and ensuring that diverse data are gathered, the COMMONS will help researchers gain a far better understanding of the intricacies of real-world Internet conditions.

3. Community Network Measurements

Within an attached local network, a wider variety of measurement options are both possible and expected. All of the access link measurements can also apply to links within the community network. Additionally, networks would contribute to: (1) anonymous HTTP Web proxy logs; (2) anonymous DNS statistics;[48] (3) traceroute server logs; (4) large-scale traceroute probes;[49] (5) support for other active measurement experiments as approved by the COMMONS policy review board;[50] (6) BGP peering[51] with, for example, the COMMONS-routeviews;[52] (7) anonymous or aggregated Web cache logs for analy-

---

fiber optic (as opposed to copper-based) networks. Since light (instead of electricity) is used on fiber optic networks, both passive and active monitors are specifically built for this medium.

[47] Packet tracing refers to "the monitoring and reporting a particular packet addresses or types for diagnostic purposes." NEWTON'S TELECOM DICTIONARY, *supra* note 2, at 690.

[48] DNS statistics are data collected from domain name servers, which are machines that connect IP addresses (e.g., 208.77.188.166) to specific domains (www.example.com).

[49] Traceroute is a widely used tool for determining the path of a packet through a network. Traceroute logs and probes help identify each router that a packet passes through and can be useful in determining the topology of a network and locating areas of congestion.

[50] *See* CAIDA 2007–2010 Program Plan, http://www.caida.org/home/about/progplan/progplan2007 (last visited Apr. 19, 2008).

[51] BGP Peering is peering using Border Gateway Protocol. Border Gateway Protocol is a Gateway Protocol that routers (other non-router devices also may be involved as intermediaries) employ in order to exchange appropriate levels of routing information. When BGP peer routers (routers with a TCP connection for purposes of exchanging routing information) first establish contact, they exchange full routing tables, which are maintained in Routing Information Bases. Subsequent contacts involve the transmission of incremental changes only. NEWTON'S TELECOMM Dictionary, *supra* note 1, at 160.

[52] Accurate knowledge of autonomous system ("AS") relationships is a requirement of many research tasks. CAIDA collects and analyzes, on an ongoing basis, AS-level topology and AS relationships, and provides this data for use by the community. CAIDA's data are available from 2004 to present, with one file created per week in 2006 and one per month in

sis; and (8) making tools available to community network users who individually volunteer to participate in research.[53]

4. End Host Measurements

Finally, the COMMONS will actively support the investigation of a recent methodological advance in the field of Internet measurement—peer production. Several existing measurement projects have drawn on the inspiration of SETI@Home to develop client-based measurement software for use in a peer production model.[54] This model takes advantage of end users' volunteering their hosts to the measurement infrastructure by downloading and executing measurement software that sends gathered data or statistics back to the project's central processing site.[55] Receiving data from unknown, untrusted users presents particularly daunting, though not insurmountable challenges.[56]

For active measurements, the biggest challenges are: (1) deployment to insure low impact on the infrastructure;[57] (2) prevention of use of tools for Distributed Denial of Service attacks;[58] (3) accountability of measurement source in case of operational problems;[59] (4) analysis of bias due to self-selection of sources (by volunteers);[60] and (5) validation of the integrity of resulting data.[61]

---

prior years. Each file contains a full AS graph derived from RouteViews BGP table snapshots taken at eight-hour intervals over a five-day period. The AS relationships available are customer-provider (and provider-customer in the opposite direction), peer-to-peer, and sibling-to-sibling.

[53] *See* CAIDA 2007–2010 Program Plan, *supra* note 50.

[54] *See* David P. Anderson, Jeff Cobb, Eric Korpela, Matt Lebotfsky & Dan Werthimer, *SETI@home: An Experiment in Public Resource Computing* 45 COMM. OF THE ACM 56, 56 (2002) (explaining that Search for Extraterrestrial Intelligence at Home (SETI@Home) is a project in which "[m]illions of computer owners worldwide contribute computer time to the search for extraterrestrial intelligence, performing the largest computation ever.").

[55] *See, e.g.*, NETI@home, http://www.neti.gatech.edu (last visited Apr. 4, 2008) ("NETI@home is an open-source software package, named after the widely popular SETI@home, that collects network performance statistics from end-users.").

[56] *See* Yuval Shavitt & Eran Shir, *DIMES: Let the Internet Measure Itself*, 35 COMPUTER COMM. REV. 71, 73–74 (discussing how the DIMES project utilizes volunteers whose contributions must be quantified).

[57] One of the major tasks for network researchers is to conduct their studies without causing artifacts or disruptions to existing services. Because data is traveling along the Internet backbone at the speed of light, even outages lasting a second or two can cause enormous headaches.

[58] A distributed denial of service attack often uses seemingly innocuous tools en masse to lock up a targeted server. While the tools used in the COMMONS have enormously useful potential, it is also imperative that they be built and deployed in ways that prevent their use for malicious intent.

[59] Network monitoring systems need to protect network user privacy, ensure the integrity of the data collected, and be deployed in ways that allow network operators and system administrators to oversee them in cases where problems might arise.

[60] Methodologically, data are only as good as the analyses conducted. Sampling bias

Client-side passive measurement infrastructures have all the same problems as active measurement infrastructures, but in addition, they bear formidable privacy challenges. For certain measurement questions, such as provider or application prevalence on the Internet, there is substantial material incentive to manipulate a macroscopic Internet measurement system. Thus, it is essential for both participant and researcher to trust in the integrity of the measurement.

Researchers do not yet have an in-depth understanding of the methodological problems of scaling Internet measurement paradigms to incorporate peer production. This article proposes a strategic approach toward a model for peer production of Internet measurements that cross-validates client-produced data with more trusted measurements from controlled infrastructure measurement devices. COMMONS Strategy Workshop participants expect that the next few years will serve as a transition period during which researchers can determine if the same integrity can be achieved from client-side infrastructures as is now achieved from controlled infrastructures.

B. Meta-infrastructure to Support Protected Data Sharing

Because the COMMONS will initially be composed of cooperative Internet Protocol ("IP") networks, commercial counterincentives to rapid and broad sharing of information will not frame inter-network security and communication policies. If launched, the COMMONS will establish a security response team to aid participating networks with integrating security best-practices into their network operations. The cooperative structure of the COMMONS will also allow research into areas that have proved impossible in the unregulated commercial framework. Such research areas will include: testing secure naming and routing protocols; coordinating public and private sector response to and recovery from major Internet disruption; developing fundamentally new architectural components that might emerge from the National Science Foundation's Global Environment for Networking Innovations ("GENI") program;[62]

---

needs to be ruled out (or accounted for) in order to maximize the applicability of the conclusions stemming from the COMMONS research.

[61] Due to the complexities involved in real-world data collection, it will be important to systematically verify the reliability of the data collected to ensure that conclusions drawn from the COMMONS research are valid.

[62] Nat'l Sci. Found., Global Environment for Networking Innovations (GENI), http://www.nsf.gov/cise/cns/geni (last visited Apr. 4, 2008).

> GENI is designed to allow experiments on a wide variety of problems in communications, networking, distributed systems, cyber-security, and networked services and applications. The emphasis is on enabling researchers to experiment with radical network designs in a way that is far more realistic than they can today. Researchers will be able to build their own new versions of the "net" or to study the "net" in ways that are not possible today. Compatibility, with the Internet is NOT required. The purpose of GENI

implementing state-of-the-art wireless techniques and policies to promote efficient utilization of spectrum; and economic modeling of a wide variety of end-to-end paths with particular aim toward transparent techniques to analyze capital and operating cost accounting.

Respect for user privacy is essential to CAIDA's mission and the goals of the COMMONS. COMMONS participants are acutely aware of the sensitivities involved in sharing of Internet measurements. CAIDA already participates in projects such as the Protected Repository for the Defense of Infrastructure Against Cyber Threats ("PREDICT")[63] and DatCat,[64] both of which are framed by these sensitivities. The launching of both of these projects makes this a perfect time to establish the COMMONS to leverage these preexisting projects and build a laboratory supporting Internet researchers across the country.

CAIDA's leadership will ensure that the COMMONS measurement infrastructure satisfies the measurement needs of the larger Internet research community while protecting the best interests of participating networks and geographic communities. For active measurement infrastructure, the primary concerns are often how to coordinate measurement requests from a large and diverse group of researchers, and how to ensure integrity of the data when gathered by an unknown party. On the other hand, for passive measurement infrastructure, the primary concerns are often the cost of hardware for high-speed trace collection and protected access to trace data. In both cases, an incentive-based cooperative model will help ensure that as many needs as possible are cost-effectively met.

1. The PREDICT Project: A Legal Framework to Support Protected Data Sharing

In 2004, the United States Department of Homeland Security ("DHS") recognized the need to support the calibration of cyber security tools[65]—particularly those funded by government agencies—in real world environments.[66] After extensive consultation with privacy law experts, DHS is cur-

---

> is to give researchers the opportunity to experiment unfettered by assumptions or requirements and to support those experiments at a large scale with real user populations.

GENI FAQ, http://www.geni.net/faq.html (last visited Apr. 4, 2008).

[63] Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), Operational Overview, http://www.predict.org [hereinafter PREDICT]. *See infra* Part IV.B.1.

[64] *See infra* Part IV.B.2.

[65] Examples of cyber security tools include samples of normal and malicious Internet traffic, malicious software samples, logs from machines compromised in targeted attacks, and other data to develop hardware and software that protects against and mitigates the effects of hacking attempts and malicious software.

[66] Dep't of Homeland Security, About the Cyber Security Research and Development

rently in the process of launching the PREDICT Project to allow researchers to request real-world datasets to assist their research.[67] The goal of the PREDICT Project is to facilitate the development of Internet defense technologies, products, models, and strategies.[68] DHS has made noteworthy progress in the legal and privacy aspects of infrastructure data access, specifically addressing the concerns of Internet Service Providers that want to support the research community, but are constrained by privacy concerns, laws, and policies.[69] The presence of such a framework bodes well for the viability of the COMMONS and demonstrates a flexible and participatory path to achieve both protection of privacy and support for empirical network science.

2. DatCat: Internet Measurement Data Catalog

For the past several years, CAIDA has been developing a data cataloging system for the Internet research community. Despite its necessity to scientific endeavor, data available to researchers are limited by legal, social, and technical constraints on its collection and distribution. Thus, the distribution of available data is a valuable service to the general research community. To this end, CAIDA has developed the Internet Measurement Data Catalog ("DatCat") to provide a searchable index of available data, enhance documentation of datasets via a public annotation system, and advance network science by promoting reproducible research.[70] Like the PREDICT Project, DatCat is a critical supporting infrastructure to the COMMONS.

C. Broader Impact: Economics, Regulations, and Policy

Measuring the Internet for a decade provides a reliable way to learn how economic issues impact a field's ability to make scientific progress. When the companies that own the infrastructure under study are declaring bankruptcy, measurements are scarce. Likewise, when the companies that own the infrastructure are competing against one another, whatever measurements do exist often are considered extremely sensitive or completely proprietary. Yet changing technologies, commercial strategies, and regulatory policies have brought dramatic restructuring of Internet service delivery at local, national, and global levels. Accompanying these changes are a variety of strong but conflicting

---

Center, http://www.cyber.st.dhs.gov/about.html (last visited Apr. 19, 2008).

[67] *See* PREDICT Home Page, http://www.predict.org (last visited Apr. 4, 2008).

[68] *Id.*

[69] *Id.*

[70] DatCat, Internet Measurement Data Catalog, http://www.datcat.org (last visited Mar. 25, 2008).

(and generally unverified) assertions concerning the relative feasibility, necessity, and superiority of different possible outcomes of this restructuring.

These assertions pose a grave dilemma for both researchers and policymakers. Given the increasingly critical role of information and communications technologies for national productivity, economic competitiveness, and even security, the costs of error could be grievous. Yet decision makers are often forced to operate in an information vacuum. They are often placed in the position of only having access to the information that the companies which would be affected by policy and regulatory changes are willing to share.

In the United States, both telecommunications companies and user advocates are unhappy with the current state of communications policy. Prices for services are higher than in many other industrialized nations, and broadband penetration is lower.[71] Telecommunications companies have increasing trouble attracting investment, and claim their broadband services need exemption from common carrier regulation in order to thrive.[72] Solutions tend to focus on industry-centric approaches to policy reform, such as how much price-control leverage should the government have over telecommunications carriers; how much freedom should telecommunications carriers have to price-discriminate; how much subsidization of telecommunications companies is necessary; and which entities should be forced to pay for universal service for rural areas. The dearth of Internet research makes it impossible to come up with reliable empirical answers to many of the questions to which regulators and politicians need answers. Thus, national telecommunications policy is forced to advance blindly at a time when the United States is losing its competitive broadband edge as compared to a growing number of industrialized countries. The COMMONS provides a collaborative environment for policymakers to help shape the research questions under study and offers a vital resource for regulators seeking to make decisions based upon empirical scientific research.

V. CONCLUSION

Building on the momentum from the COMMONS Strategy Workshop, outreach to community and municipal networks, particularly wireless initiatives,

---

[71] Robert D. Atkinson, *Framing a National Broadband Policy*, 16 COMMLAW CONSPECTUS 145, 146 (2007).

[72] This dynamic is probably best exemplified by the filings made by telecommunications companies during the Supreme Court *Brand X* case and proceedings at the FCC regarding Title I and Title II reclassification. *See* Nat'l Cable & Telecomm. Assoc. v. Brand X Internet Svc., 545 U.S. 967 (2005); *see also*, Eli M. Noam, *Beyond Liberalization II: The Impending Doom of Common Carriage*, 18 TELECOMM. POL'Y 435 (1994); WILLIAM JONES, THE COMMON CARRIER CONCEPT AS APPLIED TO TELECOMMUNICATIONS: A HISTORICAL PERSPECTIVE (1980), *available at* http://www.cybertelecom.org/notes/jones.htm.

has increased dramatically. In addition, CAIDA staff are identifying community networks to be involved in the first phase of the COMMONS, their measurement/data-collection capabilities, and the support resources needed to help maximize the utility of these measurements.

The COMMONS is one of the most important experiments the Internet research community has ever considered, and is an exciting and innovative partnership among industry, researchers, community organizers, network operators, fiber owners, municipalities, and policymakers. Through collaborative peering and rigorous data collection and analysis, the COMMONS facilitates both basic research and innovative improvements to the Internet. The COMMONS presents an unprecedented opportunity for establishing standards for scientific integrity for Internet research using rigorous empirical data to validate theories, models and simulations. In particular, the measurement data gathered through the COMMONS will lend unique strategic significance to National Science Foundation's GENI program. The potential outcome of this project promises researchers a clearer picture of the nature and characteristics of the current Internet than ever before possible, while informing discussions of future architectures and related design issues. The COMMONS also provides an opportunity for opening up the economics, ownership, and trust layers of Internetworking in much the same way the transport, network, and application layers of the Internet are open to innovation. At this critical juncture in telecommunications history, the COMMONS creates a much needed resource to help chart the future of the Internet.

Appendix 2

NEW AMERICA FOUNDATION

Open Technology Initiative

Broadband Truth-in-Labeling

By Robb Topolski, New America Foundation
September 24, 2009

The Open Technology Initiative of the New America Foundation is calling for Truth-in-Labeling by our nation's broadband operators. Drawn from similar useful disclosure requirements by lenders, these Broadband Truth-in-Labeling disclosure standards will give the marketplace a much-needed tool that clarifies and adds meaning to the terms and conditions of the service being offered.

Broadband subscribers are often frustrated that the actual performance of their Internet access service regularly falls far below the advertised speeds. Consumers set their expectations based on phrases like "up to 16 Mbps," and are disappointed to learn that these quotes are worthless as assurances. Currently, there is no lawful requirement for ISPs to reveal the contents of the broadband services they are providing; customers might be harmed by the invalid or ambiguous languages.

Internet Access Providers should disclose the important facts and details of the broadband offering before subscribers sign up. The disclosure should be meaningful, and failing to meet minimum standards should be treated as an important service outage (resulting in a refund or service credit to the consumer). Where there are choices between different products or providers, the disclosure should be made in a way that allows consumers to compare them. Providing clear, meaningful, comparable disclosures ultimately spurs competition between ISPs which encourages the future development of broadband technology.

Open Technology Initiative has created a sample Broadband Truth-in-Labeling disclosure below. ISPs use a standardized label to notice their customers what broadband services they are subscribing, including Internet speed, service guarantee, prices, service limits, and other related elements. The label aims at educating customers the contents of broadband services and making the broadband services more transparent to spur broadband competition, innovation and consumer welfare.

To make sure the broadband service is clearly expressed, the Broadband Truth-in-Labeling disclosure should be standardized to comprise several typical elements as indicators of broadband service quality, such as minimum expected speed and latency to the ISP's border router (where the ISP connects to the rest of the Internet) and service uptime. These minimum assurances will be supported by the ISP as guarantees in the delivery of broadband services, backed by technical support and service charge refunds or credits. In addition to the description of minimums being guaranteed of the service, the disclosure should include all applicable fees, a common description of the technology used to provide the services, any service limits such as a bandwidth cap or the application of any traffic management techniques, the length of the contract terms, and a link to all additional terms and conditions. Requirements should be established for disclosing any highly objectionable or surprising terms such as arbitration restrictions or information or data selling.

This Broadband Truth-in-Labeling disclosure must be shown to the consumer as part of the sign-up process and must be assertively presented again any time the ISP decide to alter the terms in such a way that alters the facts on the original Broadband Truth-in-Labeling disclosure.

ExampleCom Ultra 15 Mbps Broadband Truth-in-Labeling	
Advertised Speed	15 Mbps downstream/2 Mbps upstream
Service Guarantees **Services are measured from and to the border router.**	
Minimum Speed at Border Router	8Mbps downstream /384Kbps upstream
Minimum Reliability/Uptime	96%
Maximum Round-trip Latency (Delay) to Border Router	50ms
Service Guarantee Terms	Daily service credit upon request for any outages or extended periods of under-delivery of service
Prices	$44.99 monthly service $19.99 monthly for the first six months on promotion
Service Limits (List all traffic management techniques)	● Exceeding 100GB calendar week considered excessive use, subject to disconnect penalties, see http://www.examplecom.invalid/excessive ● Traffic by heavy users in congested areas is artificially slowed, see http://www.examplecom.invalid/shaping
Other Fees (ISPs cannot charge if not listed)	$3 monthly modem rental fee $59.99 installation fee $19 outlet installation $150 early termination during promotion period $2 account change fee $35 service call fee unless $3 monthly inside wiring maintenance plan is in force Sales taxes and franchise fees, vary by location
Contract Term	At will, customer may cancel at anytime after first six months. During the first six months, a cancellation results in a $150 fee.
Service Technology	DOCSIS 1.1 / 2.0 HFC
Legal and Privacy Policies	http://www.examplecom.invalid/legal

Appendix 3

verizon

A HIGH SPEED OFFER
THAT'S MOVING FAST.

SPECIAL INTRODUCTORY OFFER
$19.99 a month for the first 6 months, up to 3 Mbps

OFFER EXPIRES
12/31/08

Last chance to go faster.
This holiday season get faster Internet for only **$19.99** a month for the first six months. Verizon High Speed Internet gives you speeds up to 3 Mbps at an amazing value. And when you're moving up to 55 times faster than 56 Kbps dial-up, you'll do it all quicker — from downloading purchased music and videos, to holiday shopping and exchanging the season's favorite photos.

Get more than just speed.
According to *PC Magazine*'s 2008 Readers' survey, "Verizon High Speed Internet beats the average cable provider in reliability." That's because this isn't just about speed. It's about a better online experience — from setup to surfing:

- **Easy 3-step installation — so you're up and running in no time**
- **A dedicated line from our central office to your home — so even if your neighbors are online, it won't slow you down**
- **All the reliability of the Network**
- **24/7 technical support that's just a phone call away**
- **It's the best value in broadband**

To go fast you need to move fast — offer ends 12/31/08.
December 31, 2008 is your last opportunity to get Verizon High Speed Internet at 3 Mbps for only **$19.99** a month (plus taxes and fees) for the first six months; $31.99 a month for months 7–12, with a one-year agreement (plus taxes and fees). Verizon High Speed Internet is provided over the Network that gives you more.

Offer ends soon so don't wait.
CALL 1.866.905.6296 (Mon.–Sun., 7am–12am ET)

verizon.com/hotoffer19

It's the Network

Offer valid through 12/31/08. For new residential Verizon High Speed Internet customers with Verizon voice service. Rates may change after first year. $79 early termination fee. One-time charges of up to $55.00. Other charges and terms apply. Service availability and speeds may vary. ©2008 Verizon.

A mailed advertisement from Verizon boasting a $19.99 price for DSL Internet service. This priced does not accurately reflect the true price. The fine print reveals that this is a promotional, contingent on a one-year contract, there is a one time charge of "up to $55," and a consumer must also subscribe to Verizon telephone service for an additional charge in order to receive the promotional rate. Additional taxes and fees are included in the billing but these amounts are not specified in the advertisement.

Appendix 4

Exhibit A

Verizon Internet Access Terms of Service

VERIZON ONLINE TERMS OF SERVICE

PRINT >

This Agreement is between you as our Subscriber and Verizon Online LLC (or its affiliates listed in Section 16 ("Verizon" or "Verizon Online")) and it sets forth the terms and conditions under which you agree to use and we agree to provide the Service.

THIS IS A CONTRACT. PLEASE READ THESE TERMS CAREFULLY. IF YOU DO NOT AGREE TO THESE TERMS DO NOT USE THE SERVICE AND CONTACT US IMMEDIATELY TO TERMINATE IT.

1. **Term and Acceptance of Agreement; Agreement Terms Generally Included.**

   The term of this Agreement will be either month-to-month or for the term specified for the Service or Bundled Service plan you select (the "Term"). The Term begins when you accept this Agreement and ends when you or we terminate this Agreement as permitted herein.

   Acceptance by you of this Agreement occurs upon the earlier of: (a) your acceptance of this Agreement electronically during an online order, registration or when installing the Software or the Equipment; (b) your use of the Service; or (c) your retention of the Software or Equipment we provide beyond thirty (30) days following delivery. If you change Service plans, your term and monthly rate may change (depending on the plan you select), but all other provisions of this Agreement will remain in effect unless otherwise noted.

   This Agreement consists of the terms below, plus (a) the specific elements of your Service or Bundled Service plan (including the plan's pricing, duration and applicable Early Termination Fee ("ETF"), all as described in the information made available to you when placing and confirming your order); (b) our Acceptable Use Policy (Attachment A) and Additional Services Terms (Attachment B); and (c) other Verizon policies referred to in this Agreement (including our Privacy Policy), all of which are incorporated herein by reference. A current version of this Agreement and related policies are posted online at http://www2.verizon.net/policies/ ("Website"). You can also receive a paper copy of this Agreement by writing to Verizon, 14025 Riveredge Drive, Tampa, FL 33637, Attention: Customer Service.

2. **DEFINITIONS AND CHANGES TO SERVICE.**

   1. "Broadband Services" means Verizon's FiOS or DSL-based Internet services (whichever applies). Verizon's DSL-based Internet service is also known as "High Speed Internet" ("HSI").

   2. "Bundled Service(s)" means a combination or "bundle" of a Broadband Service with one or more other eligible Verizon services, including but not limited to Verizon FiOS TV, Verizon Freedom Value or Verizon Freedom Essentials, FiOS Digital Voice or Verizon ONEBILL service.

   3. "Content" means content provided by Verizon or its third party licensors or suppliers and accessible on the Service, including without limitation images, photographs, animations, video, audio, music, and text in any format.

   4. "Equipment" means the modem, router and/or other equipment provided by Verizon for use with the Service.

   5. "Service" means all Verizon dial-up, Broadband Service and Wi-Fi wireless Internet access services (where applicable), Software, Equipment, Content, Additional Services as defined in Attachment B, technical support, email, domain name server ("DNS") and related services, Verizon Web Sites and other products and services provided by Verizon under the pricing plan applicable to your Service. The

Service does not include voice telephony services.

6. "Verizon Web Site(s)" mean the sites located at http:/www.verizon.net, which are comprised of various web pages, tools, information, software, content, and features operated by Verizon.

3. **REVISIONS TO THIS AGREEMENT.**

   From time to time we will make revisions to this Agreement and the policies relating to the Service. We will provide notice of such revisions by posting revisions to the Website Announcements page, or sending an email to your primary verizon.net email address, or both. You agree to visit the Announcements page periodically to review any such revisions. We will provide you with at least thirty (30) days notice prior to the effective date of any increases to the monthly price of your Service or Bundled Service plan (excluding other charges as detailed in Sections 8.1(a)-(d)); revisions to any other terms and conditions shall be effective on the date noted in the posting and/or email we send you. By continuing to use the Service after revisions are effective, you accept and agree to abide by them.

4. **AUTHORIZED USER, ACCOUNT USE, AND RESPONSIBILITIES.**

   1. You acknowledge that you are eighteen (18) years of age or older and that you have the legal authority to enter into this Agreement. You agree promptly to notify Verizon whenever your personal or billing information changes.

   2. You are responsible for all use of your Service and account, whether by you or someone using your account with or without your permission, including all secondary or sub-accounts associated with your primary account, and to pay for all activity associated with your account. You agree to comply with all applicable laws, regulations and rules regarding your use of the Service and to only use the Service within the United States (unless otherwise permitted by this Agreement).

   3. **Restrictions on Use.** The Service is a consumer grade service and is not designed for or intended to be used for any commercial purpose. You may not resell the Service, use it for high volume purposes, or engage in similar activities that constitute such use (commercial or non-commercial). If you subscribe to a Broadband Service, you may connect multiple computers/devices within a single home to your modem and/or router to access the Service, but only through a single Verizon-issued IP address. You also may not exceed the bandwidth usage limitations that Verizon may establish from time to time for the Service, or use the Service to host any type of server. Violation of this section may result in bandwidth restrictions on your Service or suspension or termination of your Service.

   4. **Dial-Up Accounts.** If you subscribe to Dial-up Service, your Service may be subject to log-off automatically and without notice if your account is idle for fifteen minutes. An account session may be deemed to be idle if there appears to be no interactive, human generated data received from your computer system within a prescribed amount of time. Use of automatic re-dialer, script or other programs for the purpose of avoiding inactivity disconnects is a violation of this Agreement. You may only use your account for one log-on session per connection type at a time and you may not use more than one IP address for each log-on session.

   5. **Broadband Accounts.** Additional User IDs provided for Broadband customers' email boxes may not be used as dial-up connections.

5. **PRIVACY POLICY; LEGAL COMPLIANCE.**

   Personal information you provide to Verizon is governed by our Privacy Policy, which is posted on the Website and is subject to change from time to time. Verizon reserves the right to provide account and user information, including email, to third parties as required or permitted by law (such as in response to a subpoena or court order), and to cooperate with law enforcement authorities in the investigation of any criminal or civil matter. Such cooperation may include, but is not limited to, monitoring of the Verizon network consistent with applicable law. In addition, Verizon is required by law to report any facts or circumstances reported to us or that we discover from which it appears there may be a violation of the child pornography laws. We reserve the right to report any such information, including the identity of users, account information, images and other facts to law enforcement personnel.

6. **AVAILABILITY OF AND CHANGES TO SERVICE.**

1. **Service and Bandwidth Availability and Speed. The Service you select may not be available in all areas or at the rates, speeds, or bandwidth generally marketed, and some locations may not qualify for the Service even if initial testing showed that your line was qualified. We will provision qualified HSI lines at the maximum line rate available to your location based on our standard line qualification procedures, unless you have selected a level of service with a lower maximum line rate. Bandwidth is provided on a per-line (not a per-device) basis. The bandwidth available to each device connected to the network will vary depending upon the number, type and configuration of devices using the Service and the type of use (e.g., streaming media), among other factors. The speed of the Service will vary based on network or Internet congestion, your computer configuration, the condition of your telephone line and the wiring inside your location, among other factors.** We and our suppliers reserve the right, at any time, with or without prior notice to you, to restrict or suspend the Service to perform maintenance activities and to maintain session control.

2. **Changes to your local voice telephony service.** If you change your local telephone company or discontinue your local telephone service, we may in our discretion either terminate your Service or continue to provide Broadband Service without local Verizon voice service at the then-current rates, terms and conditions applicable to your new Service plan and you agree to pay any new or higher monthly fee that may apply to your new Service plan. If we elect to terminate your Service under this Section 6.2, then we reserve the right to charge any early termination fees and to apply the Equipment return terms under Section 9.

3. **Conversion from DSL Service to Verizon FiOS Internet Service.** When Verizon is able to provision Service utilizing fiber optic technologies, we may in our discretion terminate your DSL Service and cease offering DSL Service to your location. In such case, we will offer you Verizon FiOS Internet Service at the then applicable rates and terms, which may differ from your previous DSL Service rates and terms. . If you are on a Term Plan and Verizon terminates or ceases to offer service to your location under this Section 6.3, you shall not be liable to pay the ETF.

4. **Changes to Service or Features.** Verizon reserves the right to change any of the features, Content or applications of the Service at any time with or without notice to you. This includes the portal services we may make available as part of the Service or for an additional charge.

7. **SOFTWARE LICENSES AND THIRD PARTY SERVICES.**

1. We may provide you, for a fee or at no charge, software for use in connection with the Service which is owned by Verizon or its third party licensors, providers and suppliers ("Software"). We reserve the right periodically to update, upgrade or change the Software remotely or otherwise and to make related changes to the settings and software on your computer or Equipment, and you agree to permit such changes and access to your computer and Equipment. You may use the Software only in connection with the Service and for no other purpose.

2. Certain Software may be accompanied by an end user license agreement ("EULA") from Verizon or a third party. Your use of the Software is governed by the terms of that EULA and by this Agreement, where applicable. You may not install or use any Software that is accompanied by or includes a EULA unless you first agree to the terms of the EULA.

3. For Software not accompanied by a EULA, you are hereby granted a revocable, non-exclusive, non-transferable license by Verizon or its applicable third party licensor(s) to use the Software (and any corrections, updates and upgrades thereto). You may not make any copies of the Software. You agree that the Software is confidential information of Verizon or its third party licensors and that you will not disclose or use the Software except as expressly permitted herein. The Software contains copyrighted material, trade secrets, patents, and proprietary information owned by Verizon or its third party licensors. You may not de-compile, reverse engineer, disassemble, attempt to discover any source code or underlying ideas or algorithms of the Software, otherwise reduce the Software to a human readable form, modify, rent, lease, loan, use for timesharing or service bureau purposes, reproduce, sublicense or distribute copies of the Software, or

otherwise transfer the Software to any third party. You may not remove or alter any trademark, trade name, copyright or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software. You are not granted any title or rights of ownership in the Software. You acknowledge that this license is not a sale of intellectual property and that Verizon or its third party licensors continue to own all right, title and interest, including but not limited to all copyright, patent, trademark, trade secret, and moral rights, to the Software and related documentation, as well as any corrections, updates and upgrades to it. The Software may be used in the United States only, and any export of the Software is strictly prohibited.

4. Your license to use the Software or any Additional Services will remain in effect until terminated by Verizon or its third party licensors, or until your Service is terminated. Upon termination of your Service, you must cease all use of and immediately delete the Software from your computer.

5. If you subscribe to or otherwise use any third party services offered by Verizon, your use of such services is subject to the EULA of that third party provider. Violation of those terms may, in our sole discretion, result in the termination of your Service.

6. All title and intellectual property rights (including without limitation, copyrights, patents, trademarks and trade secrets) in and to the Verizon Web Sites (including but not limited to, related software, images, photographs, animations, video, audio, music, text, and content), are owned by Verizon, its affiliates or licensors. All title and intellectual property rights in and to the information and content which may be accessed through use of the Verizon Web Sites are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This Agreement does not grant you any rights to use such content, nor does it grant any rights to the Verizon Web Sites, other than the right to use the Verizon Web Sites according to the terms of the Agreement.

7. **Verizon Wi-Fi.** Verizon Wi-Fi Software and Services are provided by Boingo Wireless, Inc. ("Boingo").

8. **PRICING; BILLING: CHANGES TO SERVICE PLANS AND PAYMENT.**

1. **Prices and Fees; Billing.** You agree to pay the fees applicable to your Service or Bundled Service, either on a monthly or prepaid basis, as applicable, and to pay: a) applicable taxes, b) surcharges, c) recovery fees, d) telephone charges, e) activation fees, f) installation fees, g) set-up fees, h) equipment charges, i) ETFs, and j) other recurring and nonrecurring charges associated with the Service plan you have selected. The taxes, fees and other charges detailed in a)-d) above may vary on a monthly basis. Surcharges and recovery fees are not taxes and are not required by law, but are set by Verizon and may change. You also agree to pay any additional charges or fees applied to your account, including interest and charges due to insufficient credit or insufficient funds. Non-recurring charges such as set up, activation and installation fees, and equipment charges, will be included in your first bill. Monthly Service and Bundled Service recurring charges will be billed one month in advance; any usage charges will be billed in arrears. Pre-paid pricing plans for Additional Services will be billed in advance. Based on your election and subject to our approval, Verizon or its agent will bill you directly, or bill your charge card or local Verizon telephone bill (where available). IF YOU ELECT TO BE BILLED ON YOUR VERIZON PHONE BILL, BY USING THE SERVICES YOU AGREE TO HAVE ALL SERVICE CHARGES INCLUDED ON YOUR PHONE BILL. IF YOU SUBSCRIBE TO A BUNDLED SERVICE PLAN, THEN ALL OF THE SERVICES INCLUDED IN THE BUNDLED SERVICE PLAN MUST BE BILLED ON YOUR VERIZON PHONE BILL. Billing for Dial-up Service will automatically begin upon registration of your account. Billing for Broadband Services will automatically begin on the date provisioning of your Broadband Service is complete ("Service Ready Date"). Billing for Additional Services will begin on your Service Ready Date if you are also ordering a new Broadband Service. Otherwise, billing for Additional Services will begin upon submission of your order, unless otherwise noted. We may, at our election, waive any fees or charges. If you cancel any component of a Bundled Services plan, the monthly charges for the remaining services on your account will automatically convert to the applicable existing, non-discounted month-to-month service rate.

2. **Plans with Minimum Terms.** If you choose a Service or Bundled

Services plan with a minimum term commitment, you agree to maintain your Service for the term of that plan (a "Term Plan"). For Broadband Services, your Term Plan begins on the later of: (a) the date you change your existing Broadband Service plan to a Term Plan; or (b) your Service Ready Date; for Bundled Services, your Term Plan begins once all Bundled Services have been provisioned. You will begin receiving any discount associated with a Bundled Services plan once all Bundled Services have been provisioned. At the end of any Term Plan you may be given the option to select a new Term Plan. If you do not select a new Term Plan, your Service will automatically convert to a month-to-month Service plan at a monthly fee that may be higher than your current rate. If you select a new Term Plan, the terms of that plan will apply.

3. **Pre-paid Service Plans for Additional Services.** You may be given the option to select a pre-paid service plan for Additional Services ("Prepaid Service Plan") which will begin on the later of: (a) the date of your order, or (b) the date you change to the Prepaid Service Plan. There will be no refunds for Prepaid Service Plans. At the end of any Prepaid Service Plan, you may be given the option to select a new Prepaid Service Plan. If you do not select a new Prepaid Service Plan, your Service will automatically convert to the then-current month-to-month rate for the Additional Service.

4. **Money Back Guarantee.** If we provide a money back guarantee ("MBG") for your Service, it will begin on your Service Ready Date. During this MBG period you may cancel your Service and receive a full refund of all monthly, one-time and equipment charges paid to Verizon (provided you return all Equipment in good working condition). If you fail to return the Equipment, an unreturned Equipment fee will apply. ETFs will not apply to Service terminated within the MBG period. The MBG does not apply to customers who change between or renew bundle, monthly, term or other pricing plans. The MBG is limited to one per Subscriber per Service type per Service address.

5. **Discontinuation of Service for Nonpayment.** We may discontinue your Service without notice if Service charges on your telephone bill or charge card are refused for any reason, or if you fail to make payment when due or to provide us with a new charge card expiration date before the existing date expires.

6. **Late Fees.** If any portion of your bill is not paid by the due date, Verizon may charge you a late fee on unpaid balances and may also terminate or suspend your Service without notice. If your charges are billed by your Verizon local carrier, the late fee will be equal to the late payment charge that the local exchange carrier applies. Otherwise, the late fee will be the lesser of 1.5 % per month, or the highest rate permitted by law. If Verizon uses a collection agency or legal action to recover monies due, you agree to reimburse us for all expenses we incur to recover such monies, including attorneys' fees.

7. **Local Telephone, Toll and Long Distance Charges.** VERIZON IS NOT RESPONSIBLE FOR ANY CHARGES, INCLUDING BUT NOT LIMITED TO, LONG DISTANCE AND METERED LOCAL OR TOLL CHARGES INCURRED WHEN YOU ACCESS THE SERVICE. YOU SHOULD CHECK WITH THE LOCAL PHONE COMPANY TO DETERMINE WHETHER A DIAL-UP NUMBER YOU HAVE SELECTED IS A LOCAL CALL FROM YOUR LOCATION AND WHETHER ANY CHARGES APPLY. VERIZON DOES NOT GUARANTEE THAT ANY DIAL-UP ACCESS NUMBERS WE PROVIDE WILL BE A LOCAL CALL FROM YOUR LOCATION. ADDITIONAL CHARGES, WHICH MAY BE SUBSTANTIAL, APPLY TO REMOTE DIAL UP ACCESS, WHICH IS AVAILABLE FROM CERTAIN LOCATIONS ONLY.

8. **Limitation on Special Pricing Promotions.** You may only take advantage of one special pricing promotion during any consecutive twelve (12)-month period.

9. **Refundable Deposit.** We may require that you provide us with a refundable deposit, which will be specified at the time of your order ("Subscriber Deposit"). We may also require an additional deposit after activation of the Service if you fail to pay any amounts when due. Within ninety (90) days after termination of your Service, we -will return your Subscriber Deposit, less any unpaid amounts due on your account, including any amounts owed for unreturned or damaged Equipment. Amounts held on deposit will not accrue interest except as required by law.

10. **Credit Related Matters.** We may evaluate your credit history before modifying or providing you Service. In order to establish an account with us and/or obtain or modify Service, we may obtain a report from a consumer credit agency or exchange information with our affiliates in connection with determining your creditworthiness. If you fail to pay your bill, we may submit a negative credit report to a credit reporting agency, which will negatively affect your credit report.

9. **TERMINATION OR SUSPENSION OF SERVICE.**

    1. **Termination of Service.**

        1. **Subscribers with Month-to-Month Accounts.** If you are a month-to-month Service customer, either you or Verizon may terminate this Agreement any time by giving notice to the other as set forth in this Agreement. Termination by you will be effective upon your notice to us. Activation or set-up fees paid at the initiation of your Service, if any, are not refundable, except during any applicable 30-day MBG period.

        2. **Subscribers with Term Plans; Early Termination Fee.** EXCEPT AS OTHERWISE SET FORTH IN THIS AGREEMENT, IF YOUR BROADBAND SERVICE IS TERMINATED BY YOU OR BY US BEFORE COMPLETING YOUR TERM PLAN, THEN YOU AGREE TO PAY VERIZON THE ETF SET FORTH IN THE PRICING PLAN YOU HAVE CHOSEN. If you terminate Service at your location, your existing Term Plan cannot be carried over to a new Service location.

        3. **Termination and/or Suspension by Verizon.** Verizon reserves the right to change, limit, terminate, modify or temporarily or permanently cease providing the Service or any part of it with or without prior notice if we elect to change the Service or a part thereof or if you violate the terms of this Agreement. If Verizon terminates your Service under this Section 9.1.3, you must immediately stop using the Service and you will be responsible for the applicable fees and/or Equipment charges set forth in Sections 8.5, 9.1.1, or 9.1.2. If the termination is a result of violation by you of the terms of this Agreement, you also shall be liable to pay the ETF. . If Verizon terminates or ceases to offer service to your location, you shall not be liable to pay the ETF. If your Service is reconnected, a reconnection fee may apply.

    2. **Deletion of Data upon Termination.** YOU AGREE THAT IF YOUR SERVICE IS TERMINATED FOR ANY REASON, VERIZON HAS THE RIGHT TO IMMEDIATELY DELETE ALL DATA, FILES AND OTHER INFORMATION (INCLUDING EMAILS, ADDRESS BOOK AND WEB STORAGE CONTENT) STORED IN OR FOR YOUR ACCOUNT WITHOUT FURTHER NOTICE TO YOU.

    3. **Return of Equipment upon Termination.** If your Service is terminated for any reason prior to the end of the first year of service and you received Equipment at no charge from Verizon, you must return the Equipment to Verizon or you will be charged for the Equipment.

10. **MANAGEMENT OF YOUR DATA AND COMPUTER.**

    1. **Your Responsibilities Regarding Management of Your Computer and Data.** You are solely responsible for obtaining, maintaining and updating all equipment and software necessary to use the Service, and for management of your information, including but not limited to back-up and restoration of your data. YOU AGREE THAT VERIZON IS NOT RESPONSIBLE FOR THE LOSS OF YOUR DATA OR FOR THE BACK-UP OR RESTORATION OF YOUR DATA REGARDLESS OF WHETHER THIS DATA IS MAINTAINED ON OUR SERVERS OR YOUR DEVICE(S). YOU SHOULD ALWAYS BACK-UP ANY IMPORTANT INFORMATION SEPARATELY FROM DATA STORED ON VERIZON'S OR ANY THIRD PARTY'S SERVERS.

    2. **Content and Data Management by Verizon.** We reserve the right to: (a) use, copy, display, store, transmit and reformat data transmitted over our network and to distribute such content to multiple Verizon servers for back-up and maintenance purposes; and (b) block or remove any unlawful content you store on or transmit to or from any Verizon server. We do not guarantee the protection of your content or data located on our servers or transmitted across our network (or other networks) against loss, alteration or improper access.

3. **Your Responsibilities Regarding Security.** You agree that you are solely responsible for maintaining the security of your computer(s) and data, including without limitation, encryption of data and protection of your User ID, password and personal and other data. WE STRONGLY RECOMMEND THE USE (AND APPROPRIATE UPDATING) OF COMMERCIAL ANTI-VIRUS, ANTI-SPYWARE AND FIREWALL SOFTWARE.

4. **Monitoring of Network Performance by Verizon.** Verizon automatically measures and monitors network performance and the performance of your Internet connection and our network. We also will access and record information about your computer and Equipment's profile and settings and the installation of software we provide. You agree to permit us to access your computer and Equipment and to monitor, adjust and record such data, profiles and settings for the purpose of providing the Service. You also consent to Verizon's monitoring of your Internet connection and network performance, and to our accessing and adjusting your computer settings, as they relate to the Service, Software, or other services, which we may offer from time to time. We do not share information collected for the purpose of network or computer performance monitoring or for providing customized technical support outside of Verizon or its authorized vendors, contractors and agents.

11. **LIMITATIONS ON USE OF THE SERVICE.**

    1. You acknowledge and agree that Verizon (a) is not responsible for invalid destinations, transmission errors, or the corruption of your data; and (b) does not guarantee your ability to access all websites, servers or other facilities or that the Service is secure or will meet your needs.

    2. You acknowledge that the Service will allow access to information which may be sexually explicit, obscene or offensive, or otherwise unsuitable for children. You agree that the supervision of use of the Service by children is your responsibility and that Verizon is not responsible for access by you or any other users to objectionable or offensive content. VERIZON STRONGLY RECOMMENDS THE USE OF COMMERCIALLY AVAILABLE CONTENT FILTERING SOFTWARE.

    3. You understand and agree that if you type a nonexistent or unavailable Uniform Resource Locator (URL), or enter a search term into your browser address bar, Verizon may present you with an advanced web search page ("AWS Page") containing suggested links based upon the query you entered in lieu of your receiving an NXDOMAIN or similar error message. Verizon's provision of the AWS Page may impact applications that rely on an NXDOMAIN or similar error message and may override similar browser-based search results pages. If you would prefer not to receive AWS Pages from Verizon, you should follow the opt-out instructions that are available by clicking on the "About the Search Results Page" link on our AWS Page.

    4. You are not authorized to use any Verizon name or mark as a hypertext link to any Verizon Web site or in any advertising, publicity or in any other commercial manner without the prior written consent of Verizon Licensing Company.

    5. You agree that Verizon assumes no responsibility for the accuracy, integrity, quality completeness, usefulness or value of any Content, advice or opinions contained in any emails, message boards, chat rooms or community services, or in any other public services or social networks, and that Verizon does not endorse any advice or opinion contained therein, whether or not Verizon provides such service(s). Verizon does not monitor or control such services, although we reserve the right to do so.

    6. You represent that when you transmit, upload, post or submit any content, images or data using the Service you have the legal right to do so and that your use of such data or content does not violate the copyright or trademark laws or any other third party rights.

    7. Websites linked to or from the Service are not reviewed, controlled, or examined by Verizon and you acknowledge and agree that Verizon is not responsible for any losses you incur or claims you may have against the owner of third party websites. The inclusion of any linked websites or content from the Service, including websites or content advertised on the Service, does not imply endorsement of them by Verizon.

    8. If you choose to access the Verizon Web Sites from locations outside

the United States, you do so on your own initiative and you are responsible for compliance with all applicable local use controls, laws and regulations, including those relating to the transmission of technical data exported from or imported to the United States or the country in which you reside. Verizon makes no representation that materials on the Verizon Web Sites are appropriate or available for use in locations outside the United States and accessing them from territories where their contents are illegal is prohibited.

12. **WARRANTIES AND LIMITATION OF LIABILITY.**

    1. YOU ACKNOWLEDGE AND AGREE THAT THE SERVICE SUPPLIED HEREUNDER IS PROVIDED ON AN "AS IS" OR "AS AVAILABLE" BASIS, WITH ALL FAULTS. EXCEPT AS OTHERWISE SPECIFICALLY SET FORTH IN THIS AGREEMENT AND AS OTHERWISE SPECIFICALLY SET FORTH IN ANY MANUFACTURER WARRANTY FOR ANY EQUIPMENT PROVIDED BY VERIZON (BUT ONLY IF SUCH WARRANTY IS INCLUDED WITH SUCH EQUIPMENT), VERIZON (AND ITS OFFICERS, EMPLOYEES, PARENT, SUBSIDIARIES, AND AFFILIATES) (COLLECTIVELY THE "VERIZON PARTIES"), ITS THIRD PARTY LICENSORS, PROVIDERS AND SUPPLIERS, DISCLAIM ANY AND ALL WARRANTIES AND CONDITIONS FOR THE SERVICE, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NON-INFRINGEMENT, NON-INTERFERENCE, TITLE, COMPATIBILITY OF COMPUTER SYSTEMS, COMPATIBILITY OF SOFTWARE PROGRAMS, INTEGRATION, AND THOSE ARISING FROM COURSE OF DEALING, COURSE OF TRADE, OR ARISING UNDER STATUTE. ALSO, THERE IS NO WARRANTY OF WORKMANLIKE EFFORT OR LACK OF NEGLIGENCE. NO ADVICE OR INFORMATION GIVEN BY VERIZON OR ITS REPRESENTATIVES SHALL CREATE A WARRANTY WITH RESPECT TO ADVICE PROVIDED.

    2. VERIZON DOES NOT WARRANT OR GUARANTEE THAT SERVICE CAN BE PROVISIONED TO YOUR LOCATION, OR THAT PROVISIONING WILL OCCUR ACCORDING TO A SPECIFIED SCHEDULE, EVEN IF VERIZON HAS ACCEPTED YOUR ORDER FOR SERVICE. THE PROVISIONING OF SERVICE IS SUBJECT TO NETWORK AVAILABILITY, CIRCUIT AVAILABILITY, LOOP LENGTH, THE CONDITION OF YOUR TELEPHONE LINE AND WIRING INSIDE YOUR LOCATION, AND YOUR COMPUTER/DEVICE CONFIGURATION AND CAPABILITIES, AMONG OTHER FACTORS. IN THE EVENT YOUR LINE IS NOT PROVISIONED FOR ANY REASON, NEITHER YOU NOR VERIZON SHALL HAVE ANY DUTIES OR OBLIGATIONS UNDER THIS AGREEMENT (OTHER THAN YOUR OBLIGATION TO RETURN ANY VERIZON-PROVIDED EQUIPMENT).

    3. **VERIZON DOES NOT WARRANT THAT THE SERVICE OR EQUIPMENT PROVIDED BY VERIZON WILL PERFORM AT A PARTICULAR SPEED, BANDWIDTH OR DATA THROUGHPUT RATE, OR WILL BE UNINTERRUPTED, ERROR-FREE, SECURE, OR FREE OF VIRUSES, WORMS, DISABLING CODE OR CONDITIONS, OR THE LIKE.** VERIZON SHALL NOT BE LIABLE FOR LOSS OF YOUR DATA, OR IF CHANGES IN OPERATION, PROCEDURES, OR SERVICES REQUIRE MODIFICATION OR ALTERATION OF YOUR EQUIPMENT, RENDER THE SAME OBSOLETE OR OTHERWISE AFFECT ITS PERFORMANCE.

    4. IN NO EVENT SHALL THE VERIZON PARTIES OR VERIZON'S THIRD PARTY LICENSORS, PROVIDERS OR SUPPLIERS BE LIABLE FOR: (A) ANY INDIRECT, PUNITIVE, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OF REVENUE, LOSS OF PROGRAMS OR INFORMATION OR DAMAGE TO DATA ARISING OUT OF THE USE, PARTIAL USE OR INABILITY TO USE THE SERVICE, OR RELIANCE ON OR PERFORMANCE OF THE SERVICE, REGARDLESS OF THE TYPE OF CLAIM OR THE NATURE OF THE CAUSE OF ACTION, INCLUDING WITHOUT LIMITATION, THOSE ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR STRICT LIABILITY, EVEN IF VERIZON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH CLAIM OR DAMAGES, OR (B) ANY CLAIMS AGAINST YOU BY ANY OTHER PARTY.

    5. THE LIABILITY OF THE VERIZON PARTIES, OR (SUBJECT TO ANY DIFFERENT LIMITATIONS OF LIABILITY IN THIRD PARTY END USER LICENSE OR OTHER AGREEMENTS) OUR THIRD PARTY

LICENSORS, PROVIDERS OR SUPPLIERS, FOR ALL CATEGORIES OF DAMAGES SHALL NOT EXCEED A PRO RATA CREDIT FOR THE MONTHLY FEES (EXCLUDING ALL NONRECURRING CHARGES, REGULATORY FEES, SURCHARGES, FEES AND TAXES) YOU HAVE PAID TO VERIZON FOR THE SERVICE DURING THE SIX (6) MONTH PERIOD PRIOR TO WHEN SUCH CLAIM AROSE, WHICH SHALL BE YOUR SOLE AND EXCLUSIVE REMEDY REGARDLESS OF THE TYPE OF CLAIM OR NATURE OF THE CAUSE OF ACTION. THE FOREGOING LIMITATIONS SHALL APPLY TO THE FULL EXTENT PERMITTED BY LAW, AND ARE NOT INTENDED TO ASSERT ANY LIMITATIONS OR DEFENSES WHICH ARE PROHIBITED BY LAW.

6. ALL LIMITATIONS AND DISCLAIMERS STATED IN THIS SECTION 12 ALSO APPLY TO VERIZON'S THIRD PARTY LICENSORS, PROVIDERS AND SUPPLIERS, AS THIRD PARTY BENEFICIARIES OF THIS AGREEMENT.

7. THE REMEDIES EXPRESSLY SET FORTH IN THIS AGREEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDIES. YOU MAY HAVE ADDITIONAL RIGHTS UNDER CERTAIN LAWS (SUCH AS CONSUMER LAWS), WHICH DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY, OUR EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU.

13. **INDEMNIFICATION.**

You agree to defend, indemnify and hold harmless the Verizon Parties from and against all liabilities, costs and expenses, including reasonable attorneys' and experts' fees, related to or arising from your use of the Service (or the use of your Service by anyone else), (a) in violation of applicable laws, regulations or this Agreement; (b) to access the Internet or to transmit or post any message, information, software, images or other materials via the Internet; (c) in any manner that harms any person or results in the personal injury or death of any person or in damage to or loss of any tangible or intangible (including data) property; or (d) claims for infringement of any intellectual property rights arising from or in connection with use of the Service.

14. **NOTICES.**

1. Notices required under this Agreement by you must be provided to us at 14025 Riveredge Drive, Tampa, FL 33637, Attention: Customer Service in the manner set forth in the Contact Us section of the Website. Notice by Verizon to you (including notice of changes to this Agreement under Section 3) shall be deemed given when: (a) transmitted to your primary verizon.net email address; or (b) mailed via the US mail or hand-delivered to your address on file with us; or (c) when posted to the Announcements page of the Website.

2. If you send us an email, you agree that the User ID and/or alias contained in the email is legally sufficient to verify you as the sender and the authenticity of the communication.

15. **GENERAL PROVISIONS.**

1. All obligations of the parties under this Agreement, which, by their nature, would continue beyond the termination of this Agreement, including without limitation, those relating to Limitation of Liability and Indemnification, shall survive such termination.

2. Verizon will not be liable for delays, damages or failures in performance due to causes beyond its reasonable control, including, but not limited to, acts of a governmental body, acts of God, acts of third parties, fires, floods, strikes, work slow-downs or other labor-related activity, or an inability to obtain necessary equipment or services.

3. You may not assign or otherwise transfer this Agreement, or your rights or obligations under it, in whole or in part, to any other person. Any attempt to do so shall be void. We may freely assign all or any part of this Agreement with or without notice and you agree to make all subsequent payments as directed.

4. **Except as otherwise required by law, you and Verizon agree that the substantive laws of the Commonwealth of Virginia, without reference to its principles of conflicts of laws, will be applied to govern, construe and enforce all of the rights and duties of the parties arising from or relating in any way to the subject matter of**

this Agreement. YOU AND VERIZON CONSENT TO THE EXCLUSIVE PERSONAL JURISDICTION OF AND VENUE IN A COURT LOCATED IN FAIRFAX COUNTY, VIRGINIA FOR ANY SUITS OR CAUSES OF ACTION CONNECTED IN ANY WAY, DIRECTLY OR INDIRECTLY, TO THE SUBJECT MATTER OF THIS AGREEMENT OR TO THE SERVICE. Except as otherwise required by law, including Virginia laws relating to consumer transactions, any cause of action or claim you may have with respect to the Service must be commenced within one (1) year after the claim or cause of action arises or such claim or cause of action is barred.

5. Use, duplication or disclosure by any Government entity is subject to restrictions set forth, as applicable, in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, FAR 12.212, DFARS 227.7202, or in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Verizon or its licensors and suppliers. The use of Software and documentation is further restricted in accordance with the terms of this Agreement.

6. Verizon's failure at any time to insist upon strict compliance with any of the provisions of this Agreement shall not be construed to be a waiver of such terms in the future. If any provision of this Agreement is determined to be invalid, illegal or unenforceable, the remaining provisions of this Agreement shall remain in full force and effect and the unenforceable portion shall be construed as nearly as possible to reflect the original intentions of the parties.

7. This Agreement, including all Policies referred to herein and posted on the Website, constitutes the entire agreement between you and Verizon with respect to the subject matter hereto and supersedes any and all prior or contemporaneous agreements whether written or oral. No changes by you to this Agreement shall be effective unless agreed to in a writing signed by an authorized person at Verizon.

16. **Verizon Affiliates.** Services in New Jersey are provided by Verizon Online - New Jersey LLC. Services in Maryland are provided by Verizon Online - Maryland LLC. Services in Pennsylvania are provided by Verizon Online Pennsylvania Partnership.

ATTACHMENT A

ACCEPTABLE USE POLICY

1. **General Policy:** Verizon reserves the sole discretion to deny or restrict your Service, or immediately to suspend or terminate your Service, if the use of your Service by you or anyone using it, in our sole discretion, violates the Agreement or other Verizon policies, is objectionable or unlawful, interferes with the functioning or use of the Internet or the Verizon network by Verizon or other users, or violates the terms of this Acceptable Use Policy ("AUP").

2. **Specific Examples of AUP Violations.** The following are examples of conduct which may lead to termination of your Service. Without limiting the general policy in Section 1, it is a violation of the Agreement and this AUP to: (a) access without permission or right the accounts or computer systems of others, to spoof the URL, DNS or IP addresses of Verizon or any other entity, or to penetrate the security measures of Verizon or any other person's computer system, or to attempt any of the foregoing; (b) transmit uninvited communications, data or information, or engage in other similar activities, including without limitation, "spamming", "flaming" or denial of service attacks; (c) intercept, interfere with or redirect email or other transmissions sent by or to others; (d) introduce viruses, worms, harmful code or Trojan horses on the Internet; (e) post off-topic information on message boards, chat rooms or social networking sites; (f) engage in conduct that is defamatory, fraudulent, obscene or deceptive; (g) violate Verizon's or any third party's copyright, trademark, proprietary or other intellectual property rights; (h) engage in any conduct harmful to the Verizon network, the Internet generally or other Internet users; (i) generate excessive amounts of email or other Internet traffic; (j) use the Service to violate any rule, policy or guideline of Verizon; (k) use the service in any fashion for the transmission or dissemination of images containing child pornography or in a manner that is obscene, sexually explicit, cruel or racist in nature or which espouses, promotes or incites bigotry, hatred or racism; or (l) download or use the Service in Cuba, Iran, North Korea, Sudan and Syria or any other E:1 Country as designated by the Department of Commerce.

3. **Copyright Infringement/Repeat Infringer Policy.** Verizon respects the intellectual property rights of third parties. Accordingly, you may not store any material or use Verizon's systems or servers in any manner that constitutes an infringement of third party intellectual property rights, including under US copyright law. In accordance with the Digital Millennium Copyright Act (DMCA) and other applicable laws, it is the policy of Verizon to suspend or terminate, in appropriate circumstances, the Service provided to any subscriber or account holder who is deemed to infringe third party intellectual property rights, including repeat infringers of copyrights. In addition, Verizon expressly reserves the right to suspend, terminate or take other interim action regarding the Service of any Subscriber or account holder if Verizon, in its sole judgment, believes that circumstances relating to an infringement of third party intellectual property rights warrant such action. These policies are in addition to and do not affect or modify any other rights Verizon may have under law or contract. If you believe that copyrighted material has been used in violation of this policy or otherwise been made available on the Service in a manner that is not authorized by the copyright owner, its agent or the law, please follow the instructions for contacting Verizon's designated Copyright Agent as set forth in Verizon's Copyright Policy located at http://www.verizon.com/copy.html.

4. Verizon may, but is not required to, monitor your compliance, or the compliance of other subscribers, with the terms, conditions or policies of this Agreement and AUP. You acknowledge that Verizon shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Service, including but not limited to content that violates the law or this Agreement.

ATTACHMENT B

ADDITIONAL SERVICES TERMS

If you subscribe to any of the following services ("Additional Services"), the terms and conditions below apply to your use of the service(s) in addition to the terms of the Agreement.

1. **PERSONAL WEB SPACE ("PWS") AND VERIZON ONLINE BACKUP & STORAGE ("STORAGE SERVICES").**

    1. If PWS and/or Storage Services are made available as a feature of the Service, you agree that you are solely responsible for all content you store on or retrieve from such services. Additional terms and conditions applicable to Storage Services are posted on the Website and are incorporated herein by reference. You understand that we do not provide telephone technical support for PWS or Storage Services. Storage Services may be accessed from any suitable Internet connection.

    2. If you breach this Agreement, we reserve the right immediately to suspend or terminate your Service and/or an Additional Service(s) with or without notice. In such case, you agree that we may immediately delete all data, files, and other content stored on your Storage Services, including archived data, without further notice to you. **It is your responsibility to remove or copy any content stored on the Storage Services prior to closure of your account; otherwise, it may be lost.**

    3. Verizon reserves the right to access your PWS or Storage Service account at any time with or without prior notice to you and to disable access to or remove content which in our sole discretion is or reasonably could be deemed unlawful.

    4. Use Requirements for Free Storage Services Accounts ("Free Account"). If you sign up for a Free Account, you must actively use it. To "actively use" your account means to upload, download, backup or restore content to it. In the event you do not use your Free Account for a period of sixty (60) calendar days or more, then Verizon reserves the right to cancel your Free Account. We will provide notice of cancellation by email to your primary verizon.net email address. Use of your Free Account within fourteen (14) calendar days of the date of your cancellation notice will prevent cancellation of your Free Account. **It is your responsibility to remove or copy any content in your Free Account prior to cancellation or termination; otherwise, it will be lost. Verizon may, at its election, also delete archived data.**

    5. Verizon Online Backup & Sharing is provided by DigiData Corporation,

which is a third party beneficiary of this Agreement capable of enforcing its terms independently from Verizon.

2. **EMAIL AND EMAIL MESSAGING SERVICE.**

    1. **Email Service.** Use of Verizon email service is subject to Verizon's email and anti-spam policies, which include important information about limitations on use of the email service such as the storage capacity and deletion of stored messages. More information is available at on the Website and these email policies are incorporated herein by reference.

    2. **Email Security.** Verizon reserves the right in our sole discretion to provide the level of security we deem appropriate to safeguard our network and customers, and other Internet users, against Internet threats or abuses, including viruses, spam and phishing threats. These security measures may include, but are not limited to, the use of firewalls and blocklists to block potentially harmful or abusive emails or attachments, anti-spam filters, anti-virus and anti-spyware software, and blocking selected ports. **Such activities may result in the blocking, filtering or non-delivery of legitimate and non-legitimate email sent to or from your email account. By using any Verizon-provided email service, you agree that delivery and receipt of email is not guaranteed and to Verizon's use of such Internet and email security measures we in our sole discretion deem appropriate.**

    3. **Email Aliases.** Verizon will issue email aliases (alternate email addresses) based upon availability. You will surrender your alias by changing it or if your account is terminated for any reason and we will not forward emails addressed to that alias. If your Service is reinstated we cannot guarantee your alias will still be available to you.

3. **VERIZON INTERNET SECURITY SUITE ("VISS").**

    1. VISS is manufactured by Radialpoint SafeCare General Partnership located at 2050 Rue de Bleury, Suite 300, Montreal, Quebec, H3A 2J5. Radialpoint™ is a trademark of Radialpoint SafeCare Inc. (hereunder, along with Radialpoint SafeCare General Partnership, referred to as Radialpoint). The personal jurisdiction and venue provisions in Section 15.4 shall not apply to any causes of action by or against Radialpoint Inc. under or in relation to this Agreement. Radialpoint Inc. is a third party beneficiary of this Agreement capable of enforcing its terms independently from Verizon.

    2. You acknowledge and consent that Radialpoint Inc.: (i) may provide non-personally identifiable usage data collected in anonymous and aggregate form ("VISS Data") to its subcontractors in North America, for analysis of the performance of VISS, including the redundancy, reliability, and disaster recovery components of the services; and (ii) may use such VISS Data (1) to improve activation flow; and/or (2) as part of trends or reports published by Radialpoint Inc.

4. **VERIZON GAMES ON DEMAND.** Verizon Games on Demand are manufactured by Exent Technologies, Inc., which is a third party beneficiary of this Agreement capable of enforcing its terms independently from Verizon.

5. **STARZ PLAY.** Starz Play is provided by Starz Entertainment, LLC.

6. **VERIZON PREMIUM TECHNICAL SUPPORT SERVICE ("PTS").**

    1. **Service Description and Scope of Support.** PTS is a service intended to address issues outside the scope of Verizon's standard technical support. PTS includes: (a) configuration troubleshooting; (b) evaluation of and attempts to correct software, operating systems and networking issues; (c) virus/spyware support; and (d) software and peripherals support for network, video and sound cards, memory, hard drives, CD/DVD reader/writers, printers, scanners and networking equipment. All PTS services are offered in English only.

    2. **Limitations of PTS.**

        1. PTS does not support all software, hardware or Internet-related products, applications or features and we reserve the right to defer support issues to your equipment or software vendor. PTS does not include training on hardware or software use.

        2. PTS is not intended to replace the more advanced technical support that may be available from hardware or software manufacturers

3. PTS is for incident-specific troubleshooting and problem resolution, and excludes: i) computer programming; ii) software development; iii) warranty repairs or product replacement; iv) support for Windows® 95 and earlier versions of Windows; v) support for Mac operating systems earlier than OS X; vi) problems or issues arising out of any impermissible or unauthorized use or modification of a product or vii) upgrades of firmware, software, operating systems, or applications. Use of PTS does not constitute a license to use the software, applications or equipment being supported, or an upgrade thereto. You are responsible for obtaining any necessary licenses to use your software and applications.

4. In some cases, we may not be able to diagnose or resolve a problem because of complications with your computer or its configuration. PTS is offered as a "best efforts" service and without warranty except as specifically set forth in this Agreement. We reserve the right to refuse to troubleshoot software not on our list of supported products.

5. You understand and agree that technical problems may be the result of software or hardware errors not yet resolved by the product manufacturer, and that we may not have the ability to obtain the information necessary to resolve a specific technical problem.

6. If you purchase the Thirty (30) Minute Premium Technical Support Service ("30 Minute PTS"), the Service is non-refundable. 30 Minute PTS has a maximum duration of thirty (30) minutes and must be used within twenty-four (24) hours from the time of purchase; and you must be a subscriber to Verizon High Speed Internet or Verizon FiOS Internet service.

3. **Your Responsibilities.**

1. In order for us to provide PTS, you must first confirm that you have: a) full access (including any required licenses) to the hardware and/or software that is the basis of the problem; and (b) completed a back-up of any data, software, information or other files stored on your computer disks and/or drives that may be impacted. **Verizon is not responsible for the loss, corruption or alteration of data, software or files that may result from performance of PTS by our technicians.** You also acknowledge and agree that you are the owner or authorized user of any hardware or software about which you are contacting us. PTS is only available to you and those residing at your location; PTS is not transferrable.

2. You agree to cooperate with and follow instructions provided by Verizon and acknowledge that such cooperation by you is essential to our delivery of PTS to you.

3. You hereby grant Verizon permission to view, access and modify your computer, computer (including registry) settings and any related software or peripheral equipment, including all data, hardware and software components, in order to perform PTS.

4. You are responsible for any and all restoration and reconstruction of lost or altered files, data, or programs, and for ensuring that any information or data disclosed to Verizon is not confidential or proprietary to you or any third party.

4. **Support Procedures.**

1. Purchase Terms. PTS can be purchased either: (a) for an unlimited number of Incidents for a term beginning on the date you order PTS and continuing for the duration of the plan you selected ("Term Plan"); or (b) on a per-Incident basis (the "Per-Incident Service Plan"). For the Per-Incident Service Plan, Verizon will address a single Incident (as defined in Section 6.4.2 below) which shall include follow-up calls, as reasonable and necessary, regarding the Incident. Once an Incident is resolved (as set forth in Section 6.4.3, below), you may call back and obtain assistance on the same Incident for up to seventy-two (72) hours at no additional charge, after which the Incident will be considered closed. Once an Incident has been closed by Verizon, any further calls or requests for assistance will be

considered a new Incident and additional fees will apply if you subscribe to our Per-Incident Service Plan. IF YOU PURCHASE PTS UNDER A TERM PLAN AND YOUR SERVICE IS TERMINATED BY YOU (OR BY US IF YOU BREACH THIS AGREEMENT) BEFORE COMPLETING YOUR TERM, THEN, UPON TERMINATION OF YOUR SERVICE, YOU AGREE TO PAY VERIZON AN EARLY TERMINATION FEE IN THE AMOUNT SET FORTH IN THE PLAN YOU HAVE CHOSEN.

2. "Incident" means a specific, discrete problem for which Verizon will attempt to isolate its origin to a single cause. Verizon, in its sole discretion, will determine what constitutes an Incident.

3. An Incident will be considered resolved when you receive one of the following: (a) information or advice that resolves the Incident; (b) information on how to obtain a software solution that will resolve the Incident; (c) notice that the Incident is caused by a known, unresolved issue or an incompatibility issue; (d) information that the Incident can be resolved by upgrading to a newer release of a product; (e) notice that the Incident has been identified as a hardware equipment issue; or if (f) you cannot, or elect not to, pursue the course of action we recommend.

4. Our advice to you may include steps that you will need to take before the Incident can be resolved, such as buying cables or cords, acquiring software, etc. and we will keep your service request open for future reference when you are ready to resume the process.

5. **Third Party Warranties.** Third-party equipment, software and peripheral products are covered by the warranties provided by the original manufacturer or the seller of the product. Third party warranties may vary from product to product. It is your responsibility to consult the applicable product documentation for specific warranty information. **In addition, you acknowledge that certain third party equipment or software warranties may limit or void the remedies that they offer if unauthorized persons perform support service on the equipment or software. It is your responsibility to ensure that any impact that Verizon's delivery of PTS might have on third party warranties is acceptable to you.**

6. **Customer Specific Service.** PTS is only available to you and to persons you authorize. In either case, the terms of this Agreement will apply to the PTS services we perform.

7. **LIMITATION OF LIABILITY. VERIZON'S TOTAL LIABILITY ARISING OUT OF THE PTS SERVICE, OR FROM VERIZON'S NEGLIGENCE OR OTHER ACTS OR OMISSIONS, IF ANY, SHALL BE LIMITED, AT VERIZON'S SOLE DISCRETION AND OPTION, (A) TO REPERFORMING THE PTS SERVICE, OR (B) AS SET FORTH IN SECTION 12 OF THE AGREEMENT; EXCEPT THAT, IN THE CASE OF PER-INCIDENT SERVICE PLANS, YOUR REMEDIES WILL BE LIMITED TO A REFUND OF THE CHARGES AND FEES PAID FOR THE PTS SERVICE GIVING RISE TO THE CLAIM, IF ANY. THE REMEDIES FOR A FAILURE OR BREACH OF SUCH LIMITED WARRANTY ARE EXCLUSIVE.**

V-9.6 Effective November 30, 2009

PRINT

Verizon Internet Verizon Central | Newsroom | Entertainment | Email | Shop | My Account | Support | Site Feedback
Verizon Products Verizon Wireless | Phone | TV | Small Business Center | Enterprise Business
About Us Contact Us | Advertise with Us | Careers
Verizon Online Privacy Statement | Copyright 2009 Verizon All Rights Reserved
Use of Verizon Online Internet access services and Web sites are subject to user compliance with our Policies and Terms of Service

Appendix 4

Exhibit B

Acceptable Use Policy

COMCAST ACCEPTABLE USE POLICY FOR HIGH-SPEED INTERNET SERVICES

Contents

I. Prohibited Uses and Activities
II. Customer Conduct and Features of the Service
III. Network Management and Limitations on Data Consumption
IV. Violation of this Acceptable Use Policy
V. Copyright and Digital Millennium Copyright Act Requirements

Why is Comcast providing this Policy to me?

Comcast's goal is to provide its customers with the best residential cable Internet service possible. In order to help accomplish this, Comcast has adopted this Acceptable Use Policy (the "Policy"). This Policy outlines acceptable use of the Comcast High-Speed Internet service (the "Service"). This Policy is in addition to any restrictions contained in the Comcast Agreement for Residential Services (the "Subscriber Agreement") available at **http://www.comcast.net/terms/subscriber/**. The Frequently Asked Questions ("FAQs") at **http://help.comcast.net/** include explanations of how Comcast implements and applies many of the provisions contained in this Policy. All capitalized terms used in this Policy that are not defined here have the meanings given to them in the Subscriber Agreement.

What obligations do I have under this Policy?

All Comcast High-Speed Internet customers and all others who use the Service (the "customer," "user," "you," or "your") must comply with this Policy. Your failure to comply with this Policy could result in the suspension or termination of your Service account. If you do not agree to comply with this Policy, you must immediately stop all use of the Service and notify Comcast so that it can close your account.

How will I know when Comcast changes this Policy and how do I report violations of it?

Comcast may revise this Policy from time to time by posting a new version on the Web site at **http://www.comcast.net** or any successor URL(s) (the "Comcast.net Web site"). Comcast will use reasonable efforts to make customers aware of any changes to this Policy, which may include sending e-mail announcements or posting information on the Comcast.net Web site. Revised versions of this Policy are effective immediately upon posting. Accordingly, customers of the Comcast High-Speed Internet Service should read any Comcast announcements they receive and regularly visit the Comcast.net Web site and review this Policy to ensure that their activities conform to the most recent version. You can send questions regarding this Policy to, and report violations of it at, **http://www.comcast.net/help/contact/**. To report a child exploitation incident involving the Internet, go to **http://security.comcast.net/get-help/report-a-security-threat-or-scam.aspx#childPornography**.

I. Prohibited Uses and Activities

What uses and activities does Comcast prohibit?

In general, the Policy prohibits uses and activities involving the Service that are illegal, infringe the rights of others, or interfere with or diminish the use and enjoyment of the Service by others. For example, these prohibited uses and activities include, but are not limited to, using the Service, Customer Equipment, or the Comcast Equipment, either individually or in combination with one another, to:

Conduct and information restrictions

- undertake or accomplish any unlawful purpose. This includes, but is not limited to, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violate any local, state, federal, or non-U.S. law, order, or regulation;
- post, store, send, transmit, or disseminate any information or material which a reasonable person could deem to be unlawful;
- upload, post, publish, transmit, reproduce, create derivative works of, or distribute in any way information, software or other material obtained through the Service or

otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner;
- transmit unsolicited bulk or commercial messages commonly known as “spam;”
- send very large numbers of copies of the same or substantially similar messages, empty messages, or messages which contain no substantive content, or send very large messages or files that disrupts a server, account, blog, newsgroup, chat, or similar service;
- initiate, perpetuate, or in any way participate in any pyramid or other illegal scheme;
- participate in the collection of very large numbers of e-mail addresses, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as spidering or harvesting, or participate in the use of software (including “spyware”) designed to facilitate this activity;
- collect responses from unsolicited bulk messages;
- falsify, alter, or remove message headers;
- falsify references to Comcast or its network, by name or other identifier, in messages;
- impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar fraudulent activity (for example, “phishing”);
- violate the rules, regulations, terms of service, or policies applicable to any network, server, computer database, service, application, system, or Web site that you access or use;

Technical restrictions

- access any other person's computer or computer system, network, software, or data without his or her knowledge and consent; breach the security of another user or system; or attempt to circumvent the user authentication or security of any host, network, or account. This includes, but is not limited to, accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other hosts, networks, or accounts without express permission to do so;
- use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is strictly prohibited;
- copy, distribute, or sublicense any proprietary software provided in connection with the Service by Comcast or any third party, except that you may make one copy of each software program for back-up purposes only;
- distribute programs that make unauthorized changes to software (cracks);
- use or run dedicated, stand-alone equipment or servers from the Premises that provide network content or any other services to anyone outside of your Premises local area network (“Premises LAN”), also commonly referred to as public services or servers. Examples of prohibited equipment and servers include, but are not limited to, e-mail, Web hosting, file sharing, and proxy services and servers;
- use or run programs from the Premises that provide network content or any other services to anyone outside of your Premises LAN, except for personal and non-commercial residential use;
- service, alter, modify, or tamper with the Comcast Equipment or Service or permit any other person to do the same who is not authorized by Comcast;

Network and usage restrictions

- restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the Service (except for tools for safety and security functions such as parental controls, for example), including, without limitation, posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information;
- restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation, regardless of intent, purpose or knowledge, to the Service or any Comcast (or Comcast supplier) host, server, backbone network, node or service, or otherwise cause a performance degradation to any Comcast (or Comcast supplier) facilities used to deliver the Service;
- resell the Service or otherwise make available to anyone outside the Premises the ability to use the Service (for example, through wi-fi or other methods of networking), in whole or in part, directly or indirectly. The Service is for personal and non-commercial residential use only and you agree not to use the Service for operation as an Internet service provider or for any business enterprise or purpose (whether or not for profit);
- connect the Comcast Equipment to any computer outside of your Premises;
- interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to “crash” a host; and
- accessing and using the Service with anything other than a dynamic Internet Protocol (“IP”) address that adheres to the dynamic host configuration protocol (“DHCP”). You may not configure the Service or any related equipment to access or use a static IP address or use any protocol other than DHCP unless you are subject to a Service plan that expressly permits you to do so.

II. Customer Conduct and Features of the Service

What obligations do I have under this Policy?

In addition to being responsible for your own compliance with this Policy, you are also responsible for any use or misuse of the Service that violates this Policy, even if it was committed by a friend, family member, or guest with access to your Service account. Therefore, you must take steps to ensure that others do not use your account to gain unauthorized access to the Service by, for example, strictly maintaining the confidentiality of your Service login and password. In all cases, you are solely responsible for the security of any device you choose to connect to the Service, including any data stored or shared on that device. Comcast recommends against enabling file or printer sharing unless you do so in strict compliance with all security recommendations and features provided by Comcast and the manufacturer of the applicable file or printer sharing devices. Any files or devices you choose to make available for shared access on a home LAN, for example, should be protected with a strong password or as otherwise appropriate.

It is also your responsibility to secure the Customer Equipment and any other Premises equipment or programs not provided by Comcast that connect to the Service from external threats such as viruses, spam, bot nets, and other methods of intrusion.

How does Comcast address inappropriate content and transmissions?

Comcast reserves the right 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 in violation of Sections I or II of this Policy, or otherwise harmful to Comcast's network or customers using the Service, regardless of whether this material or its dissemination is unlawful so long as it violates this Policy. 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, file transfer, blog, 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 this Policy, the Subscriber Agreement, and applicable law.

What requirements apply to electronic mail?

The Service may not be used to communicate or distribute e-mail or other forms of communications in violation of Section I of this Policy. As described below in Section III of this Policy, Comcast uses reasonable network management tools and techniques to protect customers from receiving spam and from sending spam (often without their knowledge over an infected computer). Comcast's anti-spam approach is explained in the FAQs under the topic "What is Comcast doing about spam?" located at **http://help.comcast.net/content/faq/What-is-Comcast-doing-about-spam**.

Comcast is not responsible for deleting or forwarding any e-mail sent to the wrong e-mail address by you or by someone else trying to send e-mail to you. Comcast is also not responsible for forwarding e-mail sent to any account that has been suspended or terminated. This e-mail will be returned to the sender, ignored, deleted, or stored temporarily at Comcast's sole discretion. In the event that Comcast believes in its sole discretion that any subscriber name, account name, or e-mail address (collectively, an "identifier") on the Service may be used for, or is being used for, any misleading, fraudulent, or other improper or illegal purpose, Comcast (i) reserves the right to block access to and prevent the use of any of these identifiers and (ii) may at any time require any customer to change his or her identifier. In addition, Comcast may at any time reserve any identifiers on the Service for Comcast's own purposes. In the event that a Service account is terminated for any reason, all e-mail associated with that account (and any secondary accounts) will be permanently deleted as well.

What requirements apply to instant, video, and audio messages?

Each user is responsible for the contents of his or her instant, video, and audio messages and the consequences of any of these messages. Comcast assumes no responsibility for the timeliness, mis-delivery, deletion, or failure to store these messages. In the event that a Service account is terminated for any reason, all instant, video, and audio messages associated with that account (and any secondary accounts) will be permanently deleted as well.

What requirements apply to personal web pages and file storage?

As part of the Service, Comcast provides access to personal Web pages and storage space through the Personal Web Pages and Online Storage features (collectively, the "Personal Web Features"). You are solely responsible for any information that you or others publish or store on the Personal Web Features. You are also responsible for ensuring that all content made available through the Personal Web Features is appropriate for those who may have access to it. For example, you must take appropriate precautions to prevent minors from receiving or accessing inappropriate content. Comcast reserves the right to remove, block, or refuse to post or store any information or materials, in whole or in part, that it, in its sole discretion, deems to be in violation of Section I of this Policy. For purposes of this Policy, "material" refers to all forms of communications including text, graphics (including photographs, illustrations, images, drawings, logos), executable programs and scripts, video recordings, and audio recordings. Comcast may remove or block content contained on your Personal Web Features and terminate your Personal Web Features and/or your use of the Service if we determine that you have violated the terms of this Policy.

III. Network Management and Limitations on Data Consumption

Why does Comcast manage its network?

Comcast manages its network with one goal: to deliver the best possible broadband Internet experience to all of its customers. High-speed bandwidth and network resources are not unlimited. Managing the network is essential as Comcast works to promote the use and enjoyment of the Internet by all of its customers. The company uses reasonable network management practices that are consistent with industry standards. Comcast tries to use tools and technologies that are minimally intrusive and, in its independent judgment guided by industry experience, among the best in class. Of course, the company's network management practices will change and evolve along with the uses of the Internet and the challenges and threats on the Internet.

The need to engage in network management is not limited to Comcast. In fact, all large Internet service providers manage their networks. Many of them use the same or similar tools that Comcast does. If the company didn't manage its network, its customers would be subject to the negative effects of spam, viruses, security attacks, network congestion, and other risks and degradations of service. By engaging in responsible network management including enforcement of this Policy, Comcast can deliver the best possible broadband Internet experience to all of its customers. Visit Comcast's Network Management page at **http://www.comcast.net/terms/network** for more information.

How does Comcast manage its network?

Comcast uses various tools and techniques to manage its network, deliver the Service, and ensure compliance with this Policy and the Subscriber Agreement. These tools and techniques are dynamic, like the network and its usage, and can and do change frequently. For example, these network management activities may include (i) identifying spam and preventing its delivery to customer e-mail accounts, (ii) detecting malicious Internet traffic and preventing the distribution of viruses or other harmful code or content, (iii) temporarily lowering the priority of traffic for users who are the top contributors to current network

congestion, and (iv) using other tools and techniques that Comcast may be required to implement in order to meet its goal of delivering the best possible broadband Internet experience to all of its customers.

Are there restrictions on data consumption that apply to the Service?

The Service is for personal and non-commercial residential use only. Therefore, Comcast reserves the right to suspend or terminate Service accounts where data consumption is not characteristic of a typical residential user of the Service as determined by the company in its sole discretion. Comcast has established a monthly data consumption threshold per Comcast High-Speed Internet account of 250 Gigabytes ("GB"). Use of the Service in excess of 250GB per month is excessive use and is a violation of the Policy. See the Network Management page at **http://www.comcast.net/terms/network/** for more information and to learn how Comcast applies this Policy to excessive use. Common activities that may cause excessive data consumption in violation of this Policy include, but are not limited to, numerous or continuous bulk transfers of files and other high capacity traffic using (i) file transfer protocol ("FTP"), (ii) peer-to-peer applications, and (iii) newsgroups. You must also ensure that your use of the Service does not restrict, inhibit, interfere with, or degrade any other person's use of the Service, nor represent (as determined by Comcast in its sole discretion) an overly large burden on the network. In addition, you must ensure that your use of the Service does not limit or interfere with Comcast's ability to deliver and monitor the Service or any part of its network.

If you use the Service in violation of the restrictions referenced above, that is a violation of this Policy. In these cases, Comcast may, in its sole discretion, suspend or terminate your Service account or request that you subscribe to a version of the Service (such as a commercial grade Internet service, if appropriate) if you wish to continue to use the Service at higher data consumption levels. Comcast may also provide versions of the Service with different speed and data consumption limitations, among other characteristics, subject to applicable Service plans. Comcast's determination of the data consumption for Service accounts is final.

IV. Violation of this Acceptable Use Policy

What happens if you violate this Policy?

Comcast reserves the right immediately to suspend or terminate your Service account and terminate the Subscriber Agreement if you violate the terms of this Policy or the Subscriber Agreement.

How does Comcast enforce this Policy?

Comcast does not routinely monitor the activity of individual Service accounts for violations of this Policy, except for determining aggregate data consumption in connection with the data consumption provisions of this Policy. However, in the company's efforts to promote good citizenship within the Internet community, it will respond appropriately if it becomes aware of inappropriate use of the Service. Comcast has no obligation to monitor the Service and/or the network. However, Comcast and its suppliers reserve the right at any time to monitor bandwidth, usage, transmissions, and content in order to, among other things, operate the Service; identify violations of this Policy; and/or protect the network, the Service and Comcast users.

Comcast prefers to inform customers of inappropriate activities and give them a reasonable period of time in which to take corrective action. Comcast also prefers to have customers directly resolve any disputes or disagreements they may have with others, whether customers or not, without Comcast's intervention. However, if the Service is used in a way that Comcast or its suppliers, in their sole discretion, believe violates this Policy, Comcast or its suppliers may take any responsive actions they deem appropriate under the circumstances with or without notice. These actions include, but are not limited to, temporary or permanent removal of content, cancellation of newsgroup posts, filtering of Internet transmissions, and the immediate suspension or termination of all or any portion of the Service (including but not limited to newsgroups). Neither Comcast nor its affiliates, suppliers, or agents will have any liability for any of these responsive actions. These actions are not Comcast's exclusive remedies and Comcast may take any other legal or technical actions it deems appropriate with or without notice.

Comcast reserves the right to investigate suspected violations of this Policy, including the gathering of information from the user or users involved and the complaining party, if any, and examination of material on Comcast's servers and network. During an investigation, Comcast may suspend the account or accounts involved and/or remove or block material that potentially violates this Policy. You expressly authorize and consent to Comcast and its suppliers cooperating with (i) law enforcement authorities in the investigation of suspected legal violations, and (ii) and system administrators at other Internet service providers or other network or computing facilities in order to enforce this Policy. Upon termination of your Service account, Comcast is authorized to delete any files, programs, data, e-mail and other messages associated with your account (and any secondary accounts).

The failure of Comcast or its suppliers to enforce this Policy, for whatever reason, shall not be construed as a waiver of any right to do so at any time. You agree that if any portion of this Policy is held invalid or unenforceable, that portion will be construed consistent with applicable law as nearly as possible, and the remaining portions will remain in full force and effect.

You agree to indemnify, defend and hold harmless Comcast and its affiliates, suppliers, and agents against all claims and expenses (including reasonable attorney fees) resulting from any violation of this Policy. Your indemnification will survive any termination of the Subscriber Agreement.

V. Copyright and Digital Millennium Copyright Act Requirements

What is Comcast's DMCA policy?

Comcast is committed to complying with U.S. copyright and related laws, and requires all customers and users of the Service to comply with these laws. Accordingly, you may not store any material or content on, or disseminate any material or content over, the Service (or any part of the Service) in any manner that constitutes an infringement of third party intellectual property rights, including rights granted by U.S. copyright law. Owners of copyrighted works who believe that their rights under U.S. copyright law have been infringed may take advantage of certain provisions of the Digital Millennium Copyright Act of 1998 (the "DMCA") to report alleged infringements. It is Comcast's policy in accordance with the DMCA and other applicable laws to reserve the right to terminate the Service provided to any customer or user who is either found to infringe third party copyright or other intellectual property rights, including repeat infringers, or who Comcast, in its sole discretion, believes is infringing these rights. Comcast may terminate the Service at any time with or without notice for any affected customer or user.

How do copyright owners report alleged infringements to Comcast?

Copyright owners may report alleged infringements of their works that are stored on the Service or the Personal Web Features by sending Comcast's authorized agent a notification of claimed infringement that satisfies the requirements of the DMCA. Upon Comcast's receipt of a satisfactory notice of claimed infringement for these works, Comcast will respond expeditiously to either directly or indirectly (i) remove the allegedly infringing work(s) stored on the Service or the Personal Web Features or (ii) disable access to the work(s). Comcast will also notify the affected customer or user of the Service of the removal or disabling of access to the work(s).

Copyright owners may send Comcast a notification of claimed infringement to report alleged infringements of their works to:

J. Opperman & M. Moleski
Comcast Cable Communications, LLC
701 East Gate Drive, 3rd Floor
Mount Laurel, NJ 08054 U.S.A.
Phone: 888.565.4329
Fax: 856.324.2940
Email: **dmca@comcast.net**

Copyright owners may use their own notification of claimed infringement form that satisfies the requirements of Section 512(c)(3) of the U.S. Copyright Act. Under the DMCA, anyone who knowingly makes misrepresentations regarding alleged copyright infringement may be liable to Comcast, the alleged infringer, and the affected copyright owner for any damages incurred in connection with the removal, blocking, or replacement of allegedly infringing material.

What can customers do if they receive a notification of alleged infringement?

If you receive a notification of alleged infringement as described above, and you believe in good faith that the allegedly infringing works have been removed or blocked by mistake or misidentification, then you may send a counter notification to Comcast. Upon Comcast's receipt of a counter notification that satisfies the requirements of DMCA, Comcast will provide a copy of the counter notification to the person who sent the original notification of claimed infringement and will follow the DMCA's procedures with respect to a received counter notification. In all events, you expressly agree that Comcast will not be a party to any disputes or lawsuits regarding alleged copyright infringement.

If a notification of claimed infringement has been filed against you, you can file a counter notification with Comcast's designated agent using the contact information shown above. All counter notifications must satisfy the requirements of Section 512(g)(3) of the U.S. Copyright Act.

Revised and effective: January 1, 2009

Have You Tried

- Site Index
- Horoscopes
- Community Forums
- Anti-Virus and Firewall
- Photo Center
- Help

Quick Links

- Weather
- Local
- Comcast.net Blog
- Travel
- Jobs
- Games

Cool Tools

- TV Listings
- What's On Demand?
- Free Credit Report & Score
- Mobile Email & Ringtones
- Comcast Toolbar
- Coupons

Get More

- Entertainment
- Finance
- News
- Sports
- Music
- TV

More Sites From Comcast:

Comcast.com	Comcast.net	Comcast SportsNet	DailyCandy	E! Online	Exercise TV
Fancast	Fandango	Fearnet	G4	Golf Channel	Movies.com
PBS Kids Sprout	Plaxo	Style Network	TV One	Versus	

Add Comcast Services: Faster High-Speed Internet | Digital Cable | Digital Voice | High Definition TV

© 2009 Comcast Interactive Media Privacy Policy Terms of Service Contact Us Moving? Questions About DTV? Advertise With Us **Pay My Bill**

Appendix 4

Exhibit C

Legal Notices

View printable version

- Legal Notices
- Confidentiality of Customer Proprietary Network Information
- Acceptable Use Policy
- Qwest Availability Statement List (BMG)
- Service Level Agreement
- Interstate Month-to-Month Private Line and Network Services Agreements and Exhibits
- Month-to-Month Wholesale Data Services Agreement and Exhibits
- CPE
- Qwest® Select Advantage™ Detailed Descriptions
- Professional Services
- Regulatory Documents
- Arizona Consumers
- Colorado Consumers
- Idaho Consumers
- Iowa Consumers
- Nebraska Consumers
- New Mexico Consumers
- North Dakota Consumers
- Oregon Consumers
- South Dakota Consumers
- Utah Consumers
- Washington Consumers
- Wyoming Consumers
- Network Disclosures
- Qwest High-Speed Internet® Subscriber Agreement
- Qwest High-Speed Internet® Host Service Agreement
- Qwest Choice TV & OnLine Legal Notices
- Qwest Personal Digital Vault™
- Qwest qZone User Agreement Terms of Service
- North America IP Network Peering Policy

Acceptable Use Policy

Qwest has formulated this Acceptable Use Policy ("AUP") in order to encourage the responsible use of Qwest's networks, systems, services, web sites and products (collectively, the "Qwest Network and Services") by our customers and other users of the Qwest Network and Services (collectively, "Users"), and to enable us to provide Users with secure, reliable and productive services. By using the Qwest Network and Services, Users consent to be bound by the terms of this AUP. Qwest reserves the right to modify this AUP in its discretion at any time. Such modifications will be effective when posted. Any use of the Qwest Network and Services after such modification shall constitute acceptance of such modification.

Suspension; Termination. Any User which Qwest determines to have violated any element of this AUP may be subject to a suspension or termination of service. Qwest will suspend service for violation of the AUP on the most limited basis as Qwest determines is reasonably practical under the circumstances to address the underlying violation. Qwest will attempt to notify Customer prior to suspending service for violation of the AUP (which may be via email or any other notification); provided, however, Qwest may suspend service without notice if Qwest becomes aware of a violation of any applicable law or regulation or activity, including but not limited to a violation of the AUP, that exposes Qwest to criminal or civil liability or that exposes the Qwest network or Qwest customers' network or property to harm. Such harm to a network may include, but is not limited to, risk of having an IP address placed on blacklists. Qwest may take such further action as Qwest determines to be appropriate under the circumstances to eliminate or preclude repeat violations, and Qwest shall not be liable for any damages of any nature suffered by any Customer, User, or any third party resulting in whole or in part from Qwest's exercise of its rights under this AUP.

Prohibited Conduct.

> In General. The Qwest Network and Services must be used in a manner that is consistent with the intended purpose of the Qwest Network and Services and may be used only for lawful purposes. Users shall not use the Qwest Network and Services in order to transmit, distribute or store material: (a) in violation of any applicable law or regulation, including export or encryption laws or regulations; (b) that may adversely affect the Qwest Network and Services or other Qwest customers; or (c) that may expose Qwest to criminal or civil liability. Users are prohibited from facilitating the violation of any part of this AUP or another provider's AUP, including, but not limited to transmitting, distributing, or otherwise making available any product or service that violates this AUP or another provider's AUP.
>
> Inappropriate Content. Users shall not use the Qwest Network and Services to transmit, distribute or store material that is inappropriate, as reasonably determined by Qwest, or material that is obscene (including child pornography), defamatory, libelous, threatening, abusive, hateful, or excessively violent.
>
> Intellectual Property. Material accessible through the Qwest Network and Services may be subject to protection under privacy, publicity, or other personal rights and Intellectual Property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Qwest Network and Services in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights. If you use a domain name in connection with any of the Qwest Network and Services, you must not use that domain name in violation of the trademark, service mark, or other rights of any third party.
>
> Harmful Content. Users shall not use the Qwest Network and Services to transmit, distribute or store material that may be harmful to or interfere with the Qwest Network and Services or any third party's networks, systems, services, or web sites. Such prohibited harmful content includes, but is not limited to, viruses, worms, or Trojan horses.
>
> Fraudulent/Misleading Content. Users shall not use the Qwest Network and Services to transmit or distribute material containing fraudulent offers for goods or services, or any advertising or promotional materials that contain false, deceptive, or misleading statements, claims, or representations. In addition, Users are prohibited from submitting any false or inaccurate data on any order form, contract or online application, including the fraudulent use of

- International IP Network Peering Policy
- Electronic Signatures
- Broadband Phone Service Agreement (pdf)
- IP Voice Service Guide (pdf)
- Do Not Call Policy (pdf)

credit cards.

Email and Unsolicited Messages. Users shall not use the Qwest Network and Services to transmit unsolicited e-mail messages, including, without limitation, unsolicited bulk email , where such emails could reasonably be expected to provoke complaints ("spam"). Further, Users are prohibited from using the service of another provider to send spam to promote a site hosted on or connected to the Qwest Network and Services. In addition, Users shall not use the Qwest Network and Services in order to (a) send e-mail messages which are excessive and/or intended to harass or annoy others, (b) continue to send e-mail messages to a recipient that has indicated that he/she does not wish to receive them, (c) send e-mail with forged TCP/IP packet header information, (d) send malicious e-mail, including, without limitation, "mail-bombing", (e) send or receive e-mail messages in a manner that violates the use policies of any other Internet service provider, or (f) use an e-mail box exclusively as a storage space for data.

Third Party Rules; Usenet. Users may have access through the Qwest Network and Services to search engines, subscription Web services, chat areas, bulletin boards, Web pages, USENET, or other services that promulgate rules, guidelines or agreements to govern their use. Users must adhere to any such rules, guidelines, or agreements.

Inappropriate Actions. Users shall not use the Qwest Network and Services to conduct activities that may be harmful to or interfere with the Qwest Network and Services or any third party's networks, systems, services, or Web sites, including, but not limited to, flooding, mail bombing, or denial of service attacks. Users are prohibited from violating or attempting to violate the security of the Qwest Network and Services or the computers, accounts, or networks of another party. Users are also prohibited from any activity considered a precursor to attempted security violations, including, but not limited to, any form of scanning, probing, or other testing or information gathering activity. Inappropriate activity may result in civil or criminal liability. Qwest will investigate such activity, and may involve and cooperate with law enforcement authorities in prosecuting Users involved in such activity.

Responsibility for Content. Qwest takes no responsibility for any material created or accessible on or through the Qwest Network and Services. Qwest is not obligated to monitor such material, but reserves the right to do so. Qwest will not exercise any editorial control over such material. In the event that Qwest becomes aware that any such material may violate this AUP and/or expose Qwest to civil or criminal liability, Qwest reserves the right to block access to such material and suspend or terminate any User creating, storing or disseminating such material. Qwest further reserves the right to cooperate with legal authorities and third parties in the investigation of alleged wrongdoing, including disclosing the identity of the User that Qwest deems responsible for the wrongdoing.

Violations of this AUP may be reported at the following link: abuse@qwest.net.

Revised 01-30-09

ABOUT QWEST | CAREERS AT QWEST

Copyright © 2009 Qwest | All Rights Reserved | Legal Notices | Privacy Policy

Appendix 4

Exhibit D

Acceptable Use Policy

ACCEPTABLE USE POLICY

PRINT >

1. **General Policy:** Verizon reserves the sole discretion to deny or restrict your Service, or immediately to suspend or terminate your Service, if the use of your Service by you or anyone using it, in our sole discretion, violates the Agreement or other Verizon policies, is objectionable or unlawful, interferes with the functioning or use of the Internet or the Verizon network by Verizon or other users, or violates the terms of this Acceptable Use Policy ("AUP").

2. **Specific Examples of AUP Violations.** The following are examples of conduct which may lead to termination of your Service. Without limiting the general policy in Section 1, it is a violation of the Agreement and this AUP to: (a) access without permission or right the accounts or computer systems of others, to spoof the URL, DNS or IP addresses of Verizon or any other entity, or to penetrate the security measures of Verizon or any other person's computer system, or to attempt any of the foregoing; (b) transmit uninvited communications, data or information, or engage in other similar activities, including without limitation, "spamming", "flaming" or denial of service attacks; (c) intercept, interfere with or redirect email or other transmissions sent by or to others; (d) introduce viruses, worms, harmful code or Trojan horses on the Internet; (e) post off-topic information on message boards, chat rooms or social networking sites; (f) engage in conduct that is defamatory, fraudulent, obscene or deceptive; (g) violate Verizon's or any third party's copyright, trademark, proprietary or other intellectual property rights; (h) engage in any conduct harmful to the Verizon network, the Internet generally or other Internet users; (i) generate excessive amounts of email or other Internet traffic; (j) use the Service to violate any rule, policy or guideline of Verizon; (k) use the service in any fashion for the transmission or dissemination of images containing child pornography or in a manner that is obscene, sexually explicit, cruel or racist in nature or which espouses, promotes or incites bigotry, hatred or racism; or (l) download or use the Service in Cuba, Iran, North Korea, Sudan and Syria or any other E:1 Country as designated by the Department of Commerce.

3. **Copyright Infringement/Repeat Infringer Policy.** Verizon respects the intellectual property rights of third parties. Accordingly, you may not store any material or use Verizon's systems or servers in any manner that constitutes an infringement of third party intellectual property rights, including under US copyright law. In accordance with the Digital Millennium Copyright Act (DMCA) and other applicable laws, it is the policy of Verizon to suspend or terminate, in appropriate circumstances, the Service provided to any subscriber or account holder who is deemed to infringe third party intellectual property rights, including repeat infringers of copyrights. In addition, Verizon expressly reserves the right to suspend, terminate or take other interim action regarding the Service of any Subscriber or account holder if Verizon, in its sole judgment, believes that circumstances relating to an infringement of third party intellectual property rights warrant such action. These policies are in addition to and do not affect or modify any other rights Verizon may have under law or contract. If you believe that copyrighted material has been used in violation of this policy or otherwise been made available on the Service in a manner that is not authorized by the copyright owner, its agent or the law, please follow the instructions for contacting Verizon's designated Copyright Agent as set forth in Verizon's Copyright Policy located at http://www.verizon.com/copy.html.

4. Verizon may, but is not required to, monitor your compliance, or the compliance of other subscribers, with the terms, conditions or policies of this Agreement and AUP. You acknowledge that Verizon shall have the right, but not the obligation, to pre-screen, refuse, move or remove any content available on the Service, including but not limited to content that violates the law or this Agreement.

PRINT >

Verizon Online Privacy Statement | Copyright 2009 Verizon All Rights Reserved
Use of Verizon Online Internet access services and Web sites are subject to user compliance with our Policies and Terms of Service

Appendix 5

Exhibit A

English Ελληνικά Español Français

Welcome to Measurement Lab

About Measurement Lab

Measurement Lab (M-Lab) is an open, distributed server platform for researchers to deploy Internet measurement tools. The goal of M-Lab is to advance network research and empower the public with useful information about their broadband connections. By enhancing Internet transparency, M-Lab helps sustain a healthy, innovative Internet.

When an Internet application doesn't work as expected, how can you tell whether the problem is caused by your broadband connection, the application or something else? It can be very difficult for professional network administrators, let alone average Internet users, to answer this sort of question today.

Transparency has always been an essential component of the Internet's success, and Internet users deserve to be well-informed about the performance of their broadband connections. For that to happen, researchers need resources to develop new analytical tools.

That's where M-Lab comes in.

Tools for Users

Many researchers are already developing tools that allow users to test their broadband connections by briefly communicating with a server elsewhere on the Internet. The M-Lab platform supports the development of these measurement tools.

An Open Platform for Researchers

M-Lab assists scientific research by providing widely-distributed servers and ample connectivity for researchers' use. Each tool will be allocated dedicated resources on the M-Lab platform to facilitate accurate measurements. Server-side tools will be openly licensed and operated to allow third-parties to develop their own client-side measurement software.

Better, Open Data for Everyone

All data collected via M-Lab will be made available to the research community to allow researchers to build on a common pool of network measurement data.

M-Lab today and in the future

M-Lab is only at the beginning of its development. Today, four tools are available, running on six servers in four locations. Currently, they will only be able to support a limited number of simultaneous users. A total of 36 servers will be deployed across 12 locations early in 2009.

In order to achieve its goals, M-Lab depends on the active support of additional companies, institutions and researchers, and we welcome input from anyone interested in helping the platform flourish. As more researchers, institutions and companies participate, M-Lab will able to support a wider variety of tools.

If you are an Internet user and want to run the tools, check out our Tools page.

If you are a company, institution or researcher interested in learning more about using and supporting M-Lab, learn more here.

M-Lab Partners

M-Lab was founded by the New America Foundation's Open Technology Institute, the PlanetLab Consortium, Google Inc. and academic researchers.

What is M-Lab?

About
Who We Are
FAQ
Additional Resources
Contact

Users
Researchers

Updates

Calling all researchers - M-Lab data now available on Amazon EC2
4 days 3 hours ago

New tool -- ShaperProbe now on M-Lab
14 weeks 6 days ago

Greek Regulators and Researchers Add Support for M-Lab
15 weeks 3 days ago

Measurement Lab is a partnership of the Open Technology Institute, the PlanetLab Consortium, Google Inc., and academic researchers.
Privacy Policy & Acceptable Use Policy

All original material on Measurement Lab by New America Foundation is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.
'User' and 'Researcher' front page and sidebar icons licensed under LGPL, sourced from Oxygen Refit 2-Orange icon set.

Appendix 5

Exhibit B

Measurement Lab

Active Measurement of Internet Users' Connectivity

http://www.measurementlab.net/

Sharkfest '09

Stephen Stuart, Google

June 18, 2009

Why is M-Lab?

- Research tools have a hard time serving "flash crowds" (a.k.a. "Slashdot effect")
  - Random university connectivity != industrial-grade Internet connectivity
  - Any old spare machine is not necessarily a good machine for quality data-gathering
- Research tools need help getting visibility
  - In a word: marketing. Two words: collective marketing.

What is M-Lab?

- Purpose-built active measurement platform
- Standards for machines, connectivity
  - A little consistency goes a long way
  - Control server-side congestion, CPU oversubscription
- Connect researchers to real users, real data
  - Collect user-focused tools together

Why is M-Lab, again?

- Active measurement of users' connectivity
  - Better inform user: am I really getting N megabits?
  - Better inform researcher: insight into user problems
  - Real data, not marketing numbers
- Network transparency
  - Bring data to debates that have not had data before
  - Public policy founded on research, not hyperbole

Who is M-Lab?

- Founding members
  - New America Foundation's Open Technology Institute
  - PlanetLab Consortium
  - Google
  - Researchers
- Supporting partners
  - Voxel.net

How, Where is M-Lab?

- Think "PlanetLab," with ...
  - Consistent, current-technology machines
  - Consistent, industrial-sized connection to the Internet
- Seed round (up / in-flight / being staged)
  - North America 8/0/2
  - Europe 1/1/3
  - Asia 0/0/1

Attributions

- Data and results from M-Lab's research community
  - NDT: Richard Carlson; Internet2
  - NPAD: Matt Mathis; PSC
  - Glasnost: Marcel Dischinger, Krishna Gummadi; Max Planck Institute for Software Systems
  - Pathload2: Constantine Davrolis, Partha Kanuparthy, Nachiket Deo; Georgia Tech
  - DiffProbe: Constantine Davrolis, Partha Kanuparthy; Georgia Tech

NDT

- Sophisticated speed and diagnostic test
  - Report upload, download speeds
  - Determine if problems are limiting speeds
  - Configuration: send, receive buffers
  - Infrastructure issues: duplex mismatches and the like

NDT result

```
TCP/Web100 Network Diagnostic Tool v5.5.4b
click START to begin

** Starting test 1 of 1 **
Connected to: ndt.iupui.nuq01.measurement-lab.org  --  Using IPv4 address
Checking for Middleboxes . . . . . . . . . . . . . . . . . . . Done
checking for firewalls . . . . . . . . . . . . . . . . . . . . Done
running 10s outbound test (client-to-server [C2S]) . . . . . 605.0kb/s
running 10s inbound test (server-to-client [S2C]) . . . . . 1.77Mb/s
Your Workstation is connected to a Cable/DSL modem
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected

click START to re-test
```

Packet queuing

TCP (Transmission Control Protocol) reliably transfers data between two Internet hosts. It automatically detects and recovers from errors and losses. TCP uses buffers to provide this reliability. In addition, switches and routers use buffers to handle cases where multiple input links send packets to a single output link or link speeds change (FastEthernet to DSL modem).

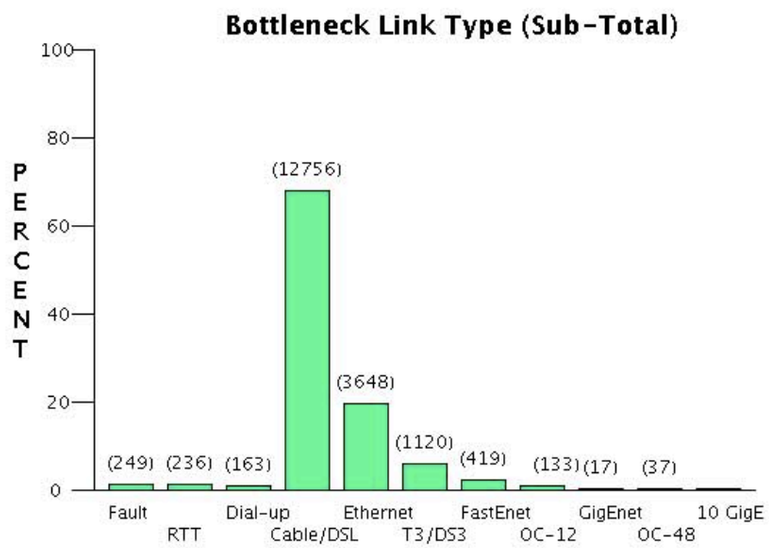
The NDT server generates and sends 10 seconds of data to the client. In some cases the server can generate data faster than it can send packets into the network (e.g., a 2 GHz CPU sending to a DSL connected client). When this happens, some packets may remain in the server output queue when the 10 second timer expires. TCP will automatically continue to send these queued packets and the client will continue to accept and process these incoming packets. This will result in the client test running longer than expected.

This condition has occurred during this test. No action is required to resolve this issue.

OK

NDT server report

NDT Usage Statistics -- Current Test Results					
Date/Time	**Total Tests**	**Bottleneck Link**	**Theoritical Limit**	**C2S Speed**	**S2C Speed**
Apr 29 14:37:57	18778	Cable Modem	429.26 Mbps	947 kbps	5424 kbps,
Packet Loss	**Average RTT**	**Mininum RTT**	**Retrans/sec**	**Timeouts/sec**	**% Out-of-Order**
None	25.95 msec	24 msec	0.00	0.00	0.00
Send Buffer	**BW*Delay**	**Receive Buffer**	**BW*Delay**	**Congestion Window**	**BW*Delay**
33554432 Bytes	10344.71 Mbps	17520 Bytes	5.40 Mbps	26280 Bytes	8.10 Mbps

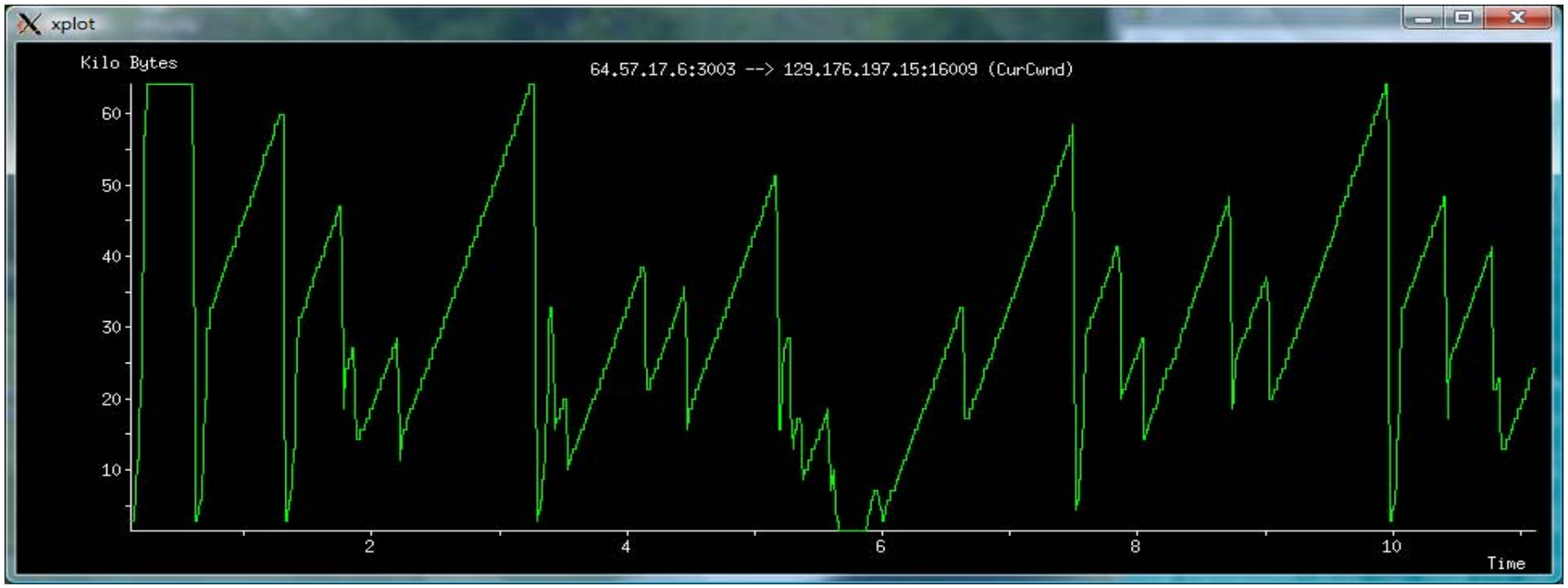


	Date/Time	Throughput Summary		Configuration Fault Summary	
Log Starts	Jan 26 22:56:04	**Client-to-Server**	**Server-to-Client**	**Duplex Mismatch**	**Excessive Errors**
Current	Apr 29 14:37:57	947 kbps	5424 kbps,	No	No
Maximum	Feb 5 15:18:22	511.61 Mbps	480.84 Mbps	5 found	0 found
Minimum	Jan 28 22:40:49	0 kbps	0 kbps		

Applet Admin started

Bottleneck link for most tests is cable modem

NDT cwnd report



TCP cwnd vs time at 5 ms increments
Slow-start to 64K limit of user's buffer
Recovery: slow-start, then congestion avoidance
Diffs in peaks may indicate competition with cross-traffic

NDT cwnd v. tcpdump

tcpdump to correlate packet events with cwnd

NDT duplex mismatch

```
TCP/Web100 Network Diagnostic Tool v5.5.4b
click START to begin

** Starting test 1 of 1 **
Connected to: ndt.iupui.nuq01.measurement-lab.org  --  Using IPv4 address
Checking for Middleboxes . . . . . . . . . . . . . . . . . . .  Done
checking for firewalls . . . . . . . . . . . . . . . . . . . .  Done
running 10s outbound test (client-to-server [C2S]) . . . . . 5.29Mb/s
running 10s inbound test (server-to-client [S2C]) . . . . . . 8.58Mb/s
The slowest link in the end-to-end path is a 10 Mbps Ethernet subnet
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected

click START to re-test
```

```
Information: Other network traffic is congesting the link
Information [S2C]: Packet queuing detected

click START to re-test

** Starting test 1 of 1 **
Connected to: ndt.iupui.nuq01.measurement-lab.org  --  Using IPv4 address
Checking for Middleboxes . . . . . . . . . . . . . . . . . . .  Done
checking for firewalls . . . . . . . . . . . . . . . . . . . .  Done
running 10s outbound test (client-to-server [C2S]) . . . . . 5.39Mb/s
running 10s inbound test (server-to-client [S2C]) . . . . . . 6.03Mb/s
The slowest link in the end-to-end path is a 10 Mbps Ethernet subnet
Alarm: Duplex Mismatch condition detected Switch=Full and Host=half
 Information [S2C]: Packet queuing detected

click START to re-test
```

NPAD

- Data rate, loss rate tests
  - Analyze TCP performance information from Web100
  - Report on factors contributing to loss/delay

NPAD result

Test conditions

Tester: 38.98.51.23 (38.98.51.23) [?]
Target: [redacted] [?]
Logfile base name: [redacted]:2009-06-15-22:57:04 [?]
This report is based on a 2 Mb/s target application data rate [?]
Warning: The section RTT is greater than the requested target RTT (73 > 70) [?]
This report is based on a 74 ms Round-Trip-Time (RTT) to the target application [?]
Original target RTT was: 70 ms. [?]
The Round Trip Time for this path section is 73.000000 ms.
The Maximum Segment Size for this path section is 1448 Bytes. [?]

Target host TCP configuration test: Pass! [?]

TCP negotiated appropriate options: WSCALE=4, SACKok, and Timestamps. [?]
The target passed all tests! See tester caveats: [?]

Path measurements [?]

The path to the tester is too long for accurate measurements.
> ***Test a shorter path section or reduce the target data rate and/or RTT. [?]***

Data rate test: Pass! [?]

Pass data rate check: maximum data rate was 2.594816 Mb/s [?]

Loss rate test: Pass! [?]

Pass: measured loss rate 0.178763% (559 packets between loss events). [?]
FYI: To get 2 Mb/s with a 1448 byte MSS on a 74 ms path the total end-to-end loss budget is 0.335570% (298 packets between losses). [?]

Suggestions for alternate tests

FYI: This path may even pass with a more strenuous application: [?]
Try rate=2 Mb/s, rtt=73 ms
Or if you can raise the MTU: [?]
Try rate=2 Mb/s, rtt=459 ms, mtu=9000 bytes

Network buffering test: Pass! [?]

This test did not complete due to other problems with the path, target or tester.
> ***Correct other problems first, and then rerun this test. [?]***
Pass: The network bottleneck has sufficient buffering (queue space) in routers and switches. [?]
Estimated queue size is at least: Pkts: 14 Bytes: 20272
This is probably an underestimate of the actual queue size. [?]
This corresponds to a 55.775042 ms drain time. [?]
To get 2 Mb/s with on a 74 ms path, you need 18500 bytes of buffer space. [?]

The network path passed all tests! [?]

Tester validation: Pass! [?]

Glasnost

- Developed to determine whether BitTorrent was being manipulated
- 25% of tested users experience degradation
  - 60% of differentiated flows have throughput reduced to .5 of reference flows
  - 40% reduced to .2 of reference flows
- Much more detail in upcoming SOSP paper

Glasnost result

Results for your host ([redacted]**:**

Is BitTorrent traffic on a well-known BitTorrent port (6881) throttled?

- **The BitTorrent upload (seeding) worked.** Our tool was successful in uploading data using the BitTorrent protocol.
  - **There's no indication that your ISP rate limits your BitTorrent uploads.** In our tests a TCP upload achieved at least 567 Kbps while a BitTorrent upload achieved at most 590 Kbps. You can find details here.
- **The BitTorrent download worked.** Our tool was successful in downloading data using the BitTorrent protocol.
  - **There's no indication that your ISP rate limits your BitTorrent downloads.** In our tests a TCP download achieved at least 1054 Kbps while a BitTorrent download achieved at most 1468 Kbps. You can find details here.

Is BitTorrent traffic on a non-standard BitTorrent port (10009) throttled?

- **The BitTorrent upload (seeding) worked.** Our tool was successful in uploading data using the BitTorrent protocol.
  - **There's no indication that your ISP rate limits your BitTorrent uploads.** In our tests a TCP download achieved at least 591 Kbps while a BitTorrent download achieved at most 599 Kbps. You can find details here.
- **The BitTorrent download worked.** Our tool was successful in downloading data using the BitTorrent protocol.
  - **There's no indication that your ISP rate limits your BitTorrent downloads.** In our tests a TCP download achieved at least 976 Kbps while a BitTorrent download achieved at most 1484 Kbps. You can find details here.

Is TCP traffic on a well-known BitTorrent port (6881) throttled?

- **There's no indication that your ISP rate limits all downloads at port 6881.** In our test, a TCP download on a BitTorrent port achieved at least 1163 Kbps while a TCP download on a non-BitTorrent port achieved at least 976 Kbps. You can find details here.
- **There's no indication that your ISP rate limits all uploads at port 6881.** In our test, a TCP upload on a BitTorrent port achieved at least 629 Kbps while a TCP upload on a non-BitTorrent port achieved at least 591 Kbps. You can find details here.

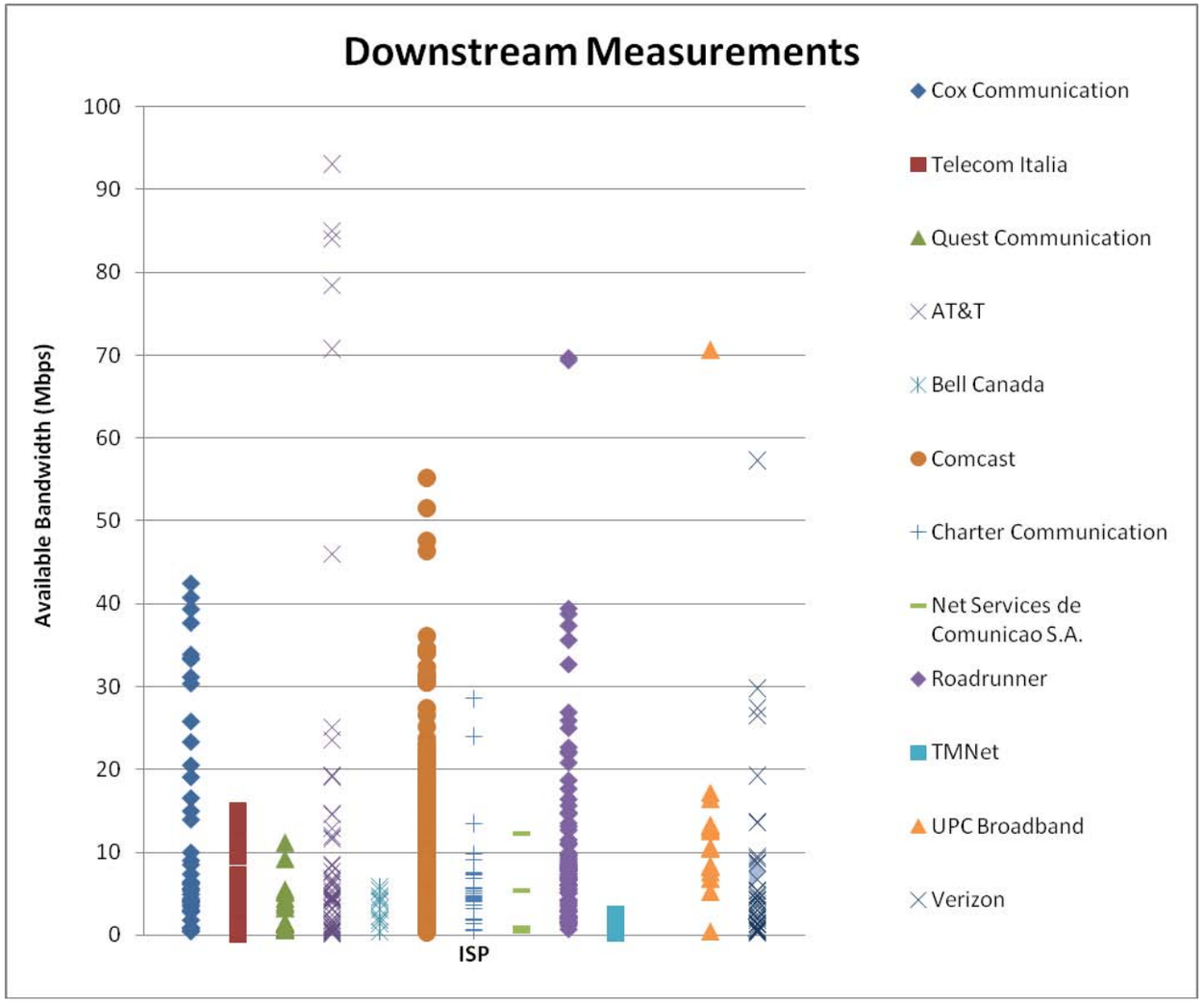
Pathload2

- Measures available bandwidth
  - Not the throughput of a large TCP flow
  - “Raw” bits per second, independent of transport or application protocol

Pathload2 result

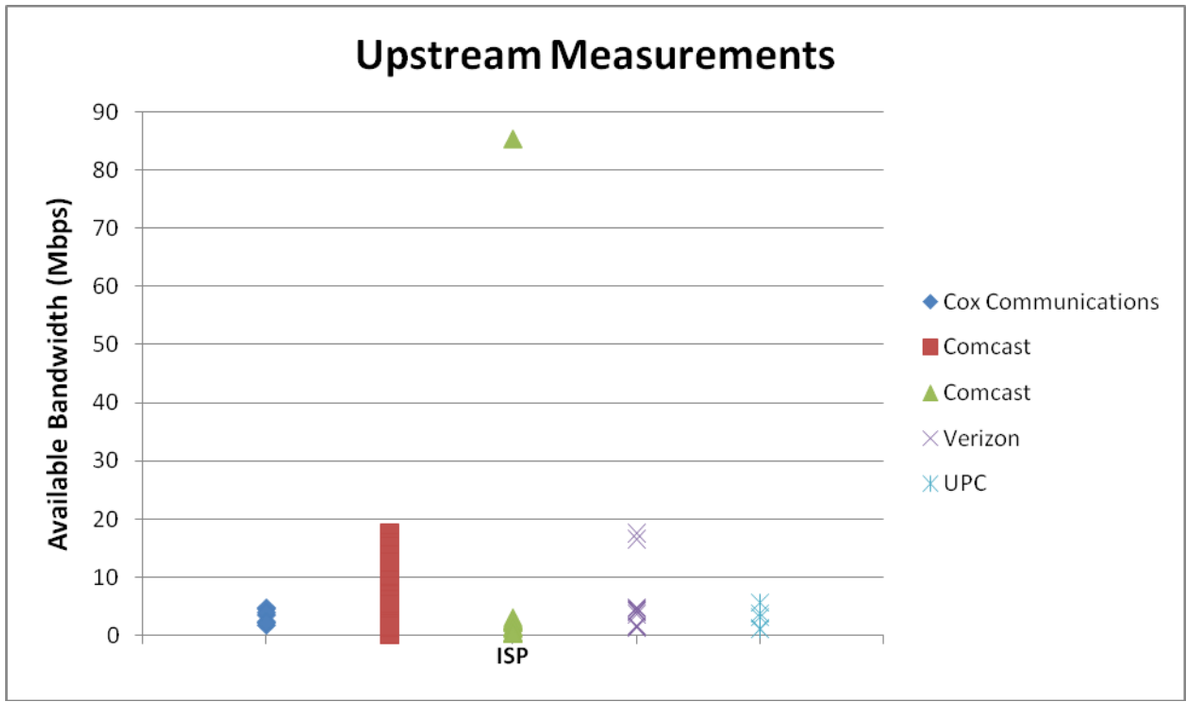
```
Last login: Mon Jun 15 15:59:48 on ttys001
Mon Jun 15 16:01:16 PDT 2009
68-26-181-33> /Volumes/Disk\ Image/pathload2 ; exit;
Connecting to selected M-lab server.
Connected to MLab Server: 74.63.50.34
Measuring Upstream Available Bandwidth
Sending fleet 0, Probing Rate 0.61 Mbps ############

Measuring Downstream Available Bandwidth
Receiving Fleet 0, Probing Rate 2.29Mbps ############
Receiving Fleet 1, Probing Rate 1.15Mbps ############
Measurement completed.

        *****  RESULT *****
Upstream Measurement (towards the Internet)
Available bandwidth is at most 0.61 (Mbps)
Measurement duration : 35.97 sec

Downstream Measurement (from the Internet)
Available bandwidth range : 0.90 - 2.30 (Mbps).
Measurement duration : 29.08 sec.

For more information about available bandwidth measurement,
please see: http://www.pathrate.org
logout

[Process completed]
```

Pathload2



Measurement of available downstream bandwidth

Pathload2



Measurement of available upstream bandwidth

DiffProbe

- Tests for discrimination
  - Priority scheduling or buffer management
  - Traffic shaping and policing
- Preliminary results
  - No discrimination of Skype, Vonage detected
  - Comcast residential traffic shaping detected; per customer, not per application/service

ShaperProbe

- First of the modules of DiffProbe, sample output:

```
DiffProbe alpha release. April 2009.
Shaper Detection Module.

Connected to server 64.9.225.153.

Estimating capacity:
Upstream: 3112 Kbps.
Downstream: 35475 Kbps.

Checking for traffic shapers:
Upstream: Burst size: 4787-4858 KB; Shaping rate: 1064 Kbps.

sending measurement data to server..done.
Downstream: Burst size: 9240-10001 KB; Shaping rate: 6346 Kbps.
```

- This is from Comcast; they call it SpeedBurst, or PowerBoost, or something
- Not “DropYourPackets” or “GoodLuckTunnelingX”

M-Lab = alpha

- New tool deployments planned
  - NANO, others in the pipeline
  - New protocols (voice? streaming video?) to provide more frames of reference
- Data to be published
  - Working on repository options
  - Goal is open access to collected datasets

Measuring is hard

- A cautionary tale that the infrastructure doesn't always do what you think would be the sensible thing
  - Traceroute from my desk to mlab1.nuq01
  - Distance as crow flies, maybe .5 miles
  - You'd think a couple milliseconds ...

Map = territory (sometimes)

- ... and you'd be right in some cases.

```
% traceroute -n mlab1.nuq01.measurement-lab.org
traceroute to mlab1.nuq01.measurement-lab.org (64.9.225.137), 64 hops max, 40 byte packets
 1  172.19.27.252  3.227 ms  1.221 ms  1.036 ms
 2  172.25.252.234  1.330 ms  1.147 ms  1.102 ms
 3  172.25.254.64  1.115 ms  1.167 ms  1.182 ms
 4  172.25.253.36  1.110 ms  1.143 ms  1.238 ms
 5  172.22.0.209  1.239 ms  1.242 ms  1.176 ms
 6  216.239.45.60  1.466 ms  1.416 ms  1.721 ms
 7  66.249.94.36  2.327 ms  2.446 ms  2.089 ms
 8  64.233.174.10  3.329 ms  3.128 ms  3.199 ms
 9  64.9.224.130  3.582 ms  3.501 ms  3.726 ms
10  64.9.224.146  4.103 ms  4.037 ms  3.871 ms
11  64.9.225.137  3.726 ms  4.019 ms  3.824 ms
```

- Not all cases, though.

Map != territory

- ~~Prisoner~~ Packet exchange happens in Los Angeles

```
% traceroute mlab1.nuq01.measurement-lab.org
traceroute to mlab1.nuq01.measurement-lab.org (64.9.225.137), 64 hops max, 40 byte packets
 1  68.28.49.85 (68.28.49.85)  53.626 ms  52.683 ms  66.902 ms
 2  68.28.49.91 (68.28.49.91)  54.884 ms  71.667 ms  72.872 ms
 3  68.28.51.54 (68.28.51.54)  74.809 ms  95.026 ms  107.125 ms
 4  68.28.55.5 (68.28.55.5)  74.821 ms  69.172 ms  74.947 ms
 5  * * *
 6  68.28.53.69 (68.28.53.69)  50.518 ms  50.022 ms  72.776 ms
 7  sl-gw10-bur-1-0-0.sprintlink.net (144.223.255.17)  75.133 ms  49.361 ms  74.114 ms
 8  sl-bb20-bur-10-0-0.sprintlink.net (144.232.0.66)  73.887 ms  72.106 ms  69.981 ms
 9  sl-crs2-ana-0-1-3-3.sprintlink.net (144.232.18.160)  73.072 ms  75.187 ms  83.850 ms
10  sl-st20-la-0-0-0.sprintlink.net (144.232.20.204)  54.939 ms
    sl-st20-la-11-0-0.sprintlink.net (144.232.8.94)  76.419 ms
    sl-st20-la-0-0-0.sprintlink.net (144.232.20.204)  78.058 ms
11  sl-st30-la-0-0-0-0.sprintlink.net (144.232.1.116)  72.891 ms  77.065 ms  74.105 ms
12  xe-7-3-0.edge1.losangeles9.Level3.net (4.68.111.169)  57.841 ms  72.220 ms  74.971 ms
13  ae-83-80.ebr3.LosAngeles1.Level3.net (4.69.144.180)  80.906 ms  77.965 ms
    ae-63-60.ebr3.LosAngeles1.Level3.net (4.69.144.52)  90.110 ms
14  ae-2.ebr3.SanJose1.Level3.net (4.69.132.9)  91.473 ms  93.197 ms  89.974 ms
15  ae-83-83.csw3.SanJose1.Level3.net (4.69.134.234)  81.750 ms  82.134 ms  88.102 ms
16  ae-32-89.car2.SanJose1.Level3.net (4.68.18.132)  87.763 ms  81.401 ms  80.137 ms
17  GOOGLE-INC.car2.SanJose1.Level3.net (4.79.42.174)  61.997 ms  81.120 ms  87.140 ms
18  64.9.224.130 (64.9.224.130)  95.821 ms  86.158 ms  86.032 ms
19  64.9.224.146 (64.9.224.146)  84.877 ms  108.308 ms  90.853 ms
20  64.9.225.137 (64.9.225.137)  89.064 ms  64.141 ms  84.113 ms
```

Map still != territory

- Using server in LAX is actually worse; seriously, this was minutes later and there's 2x RTT (and one more hop) to 68.28.53.69

```
% traceroute mlab1.lax01.measurement-lab.org
traceroute to mlab1.lax01.measurement-lab.org (38.98.51.9), 64 hops max, 40 byte packets
 1  68.28.49.85 (68.28.49.85)  73.089 ms  73.477 ms  71.892 ms
 2  68.28.49.91 (68.28.49.91)  69.014 ms  52.352 ms  72.925 ms
 3  68.28.51.55 (68.28.51.55)  73.859 ms  72.600 ms  72.902 ms
 4  * * *
 5  68.28.55.5 (68.28.55.5)  74.348 ms  73.618 ms  72.921 ms
 6  * * *
 7  68.28.53.69 (68.28.53.69)  104.433 ms  145.817 ms  104.245 ms
 8  sl-gw10-bur-1-0-0.sprintlink.net (144.223.255.17)  114.867 ms  100.362 ms  121.382 ms
 9  sl-bb20-bur-10-0-0.sprintlink.net (144.232.0.66)  87.580 ms  99.754 ms  120.988 ms
10  sl-crs2-ana-0-1-3-3.sprintlink.net (144.232.18.160)  129.888 ms  98.784 ms  113.795 ms
11  sl-st20-la-11-0-0.sprintlink.net (144.232.8.94)  122.016 ms
    sl-st20-la-0-0-0.sprintlink.net (144.232.20.204)  175.713 ms  129.921 ms
12  sl-st31-la-0-0-0-0.sprintlink.net (144.232.5.104)  172.835 ms  146.504 ms  114.911 ms
13  * * *
14  te4-2.ccr01.lax01.atlas.cogentco.com (154.54.6.229)  200.542 ms
    te7-4.ccr01.lax01.atlas.cogentco.com (154.54.3.9)  174.211 ms
    te8-1.ccr01.lax01.atlas.cogentco.com (154.54.0.213)  158.268 ms
15  te9-1.mpd01.lax01.atlas.cogentco.com (154.54.2.118)  153.434 ms  188.308 ms  134.990 ms
16  vl3811.na31.b020604-0.lax01.atlas.cogentco.com (38.20.38.154)  393.642 ms  196.608 ms
    vl3511.na31.b020604-0.lax01.atlas.cogentco.com (38.20.38.150)  213.972 ms
17  38.104.77.234 (38.104.77.234)  160.679 ms  146.274 ms  156.947 ms
18  38.98.51.9 (38.98.51.9)  147.001 ms  165.632 ms  124.812 ms
```

How can we measure at all?

- Measurement takes time, patience
  - Tempus fugit - paths, congestion conditions change rapidly, try to measure "simultaneously" to leverage similar conditions
  - Understand that the sand shifts under your feet between measurements: how much? what is a "baseline measurement?"
- More data provides more insight
  - Key development area for M-Lab - automated, scheduled test runs on the client side
  - cron is not rocket science ... and yet, it is

What can you do?

- Try the tools
  - And not just once - try to discover what is baseline versus optimal versus degraded
  - Start a conversation with researchers
- Think about tool development
  - Are you working on something that could measure against an M-Lab server?
  - Analysis/visualization tools for published data?

Where to go for more

- www.measurementlab.net

Appendix 6

Analyzing in the Dark:
The Internet Research Data Acquisition Crisis

When the NSFnet backbone was privatized in 1995 the network science community lost access to the only set of publicly available statistics on a national Internet backbone network. This transition essentially eliminated the opportunity to conduct analyses on a widely-used backbone. Today, far from having an analytic handle on the Internet, network researchers often lack the ability to measure traffic at the granularity necessary to make increasingly critical infrastructure improvements. Legislators operate under an enforced ignorance of potential security problems when the scientific community is unable to identify potential congestion points on the internet, and empirically clueless about how the Internet can be improved. Access to network traffic data would allow researchers to begin solving problems of cyber-security, spam overload, privacy invasion and identity theft, digital rights management and piracy, network congestion, pricing discrimination, illegal pornography and a host of other issues. Without these data, network scientists, regulators, and decision-makers are left fumbling in the dark as we attempt of address these seemingly intractable and growing problems.

Over the past decade, while the core of the Internet has continued to expand, scientific measurement and modeling of its systemic characteristics has largely stalled. An inevitable problem with contemporary Internet traffic measurement studies is that they are quickly made obsolete in an environment where traffic, technology, and topology change faster than we can currently measure them. The proliferation of multimedia content and new services and applications makes the acquisition of data far more difficult and costly than in previous years. Much like a scanning electron microscope is a critical tool for modern physics laboratories, high-powered and expensive measurement tools are needed by Internet researchers to keep pace with the Internet's increasing complexity.

These problems have recently been identified by the Department of Homeland Security (DHS) as critically important to the longterm interests and security of the United States. Recently, DHS recognized the need to support the calibration of cyber-security tools in real world environments and has launched the PREDICT Project to allow researchers to request datasets to assist their research into cyber-defense technologies, products, models and strategies. DHS has facilitated progress in the legal and privacy facets of infrastructure data access, specifically addressing the concerns of Internet Service Providers who want to support the research community but are constrained by privacy laws or policies. However, while DHS is actively supporting the sharing of existing datasets for research and analysis, it has no budget for conducting research on the infrastructure itself. Meanwhile, the National Science Foundation has cut measurement infrastructure project budgets by 75% or more due to funding constraints, thus exacerbating the problem.

We cannot hope to build a national broadband policy that brings America into the digital future without a solid understanding of what is happening on our networks. Throughout the decades that the United States government was steward of the early Internet, the only statistics collected regularly were those required by government contract. Since the privatization of the Internet in the mid-1990s, we have embraced a policy that has sacrificed this data access, assuming that the less regulation of the Internet, the better. What is absolutely clear, however, is that this privatization has created disastrous outcomes for network science and basic research due to the lack of regulatory requirements for transparency. Because of the pervasiveness of non-disclosure agreements and the practice of treating even mundane operational practices as trade secrets, today's network science operates in a self-perpetuating “fog of unknowing” around the Internet.

The Internet Data Acquisition Crisis is multifaceted and includes numerous mission-critical elements that network researchers cannot measure. Taken together, these "unknowns" are creating clear national security concerns by undermining our knowledge about this critical information infrastructure. Notable topic areas researchers are particularly concerned about include:

- network topology from one point to another (in either direction, at any network layer);
- propagation of a routing update across the Internet (i.e., how robust routing is);
- core router information such as their Router Information Base (RIB) – researchers can only gain access to a router's Forwarding Information Base (FIB);
- precise one-way delay from two places on the Internet (i.e., how efficient the routing is);
- hour packet information in the Internet's core (e.g., the collection of packet traces, even anonymized, from any backbone available to any academic researcher);
- accurate flow counts from the Internet's core (i.e., how much throughput);
- anything from the Internet's core with real IP addresses (e.g., where data is coming from/to);
- the topology of the Internet's core (i.e., how does the Internet's core interconnect);
- accurate bandwidth or capacity information – not even along a path, much less for each link (i.e., link performance information);
- how much, in absolute or relative terms, spam/phishing/viruses/botnets/hosts/routers exists;
- information on what is causing problems (e.g., the existence of obsolete or misconfigured software, network and protocol parameters, bad cables, lossy media, insufficient send/receive buffers, route instability, VPNs, firewalls);
- cost structure data; and,
- potential privacy/legal issues in the Internet's operations.

Important questions researchers cannot answer due to this Data Acquisition Crisis:

- What percent of Internet users in the US (or world) are running p2p file sharing applications?
- What proportion of traffic going across a given network backbone is: spam, malware (botnets, worms, phishing), encrypted, or real-time? How fast are these categories growing? How much overhead do they represent on the network? How do they shift the economics of the network?
- What are the effects of outages, new routing policies, and other topology changes on surrounding (or distant) Internet Service Providers (ISPs)?
- Which providers control how much Internet topology/bandwidth resources in the US?
- Which segments of the infrastructure are especially vulnerable (or subject) to congestion?
- What is the extent of asymmetric routing and route instability as a function of ISP and over time? What is the impact of asymmetry on performance?
- What are the root causes of Internet outages, and how does the distribution change over time?
- How effectively are we utilizing IPv4 address space (projected to be used up in 3-5 years) and BGP routing table space?
- How efficiently does the Internet backbone move traffic around? What percent of traffic is unwanted by the destination receiving it? What artificial bottlenecks exist?

Critical research areas scientists cannot pursue because of this Data Acquisition Crisis:

- Sustainable interdomain routing and addressing architecture (particularly important since we will run out of IPv4 addresses within the next half-decade).
- Improvements in congestion control. It is widely recognized that the most prevalent data transport protocol in the Internet, TCP, is not behaving efficiently at modern bandwidths and for real-time applications such as voice.
- Measurement technology itself – it is difficult to justify investing resources into measurement technology when there is no promise of a network (or traffic, on a testbed) to measure.
- Innovative security, multimedia, and IP transport technologies (e.g., DNSSEC, S-BGP, multicast, RSVP/QOS).