ORAL ARGUMENTS SCHEDULED DECEMBER 4, 2015
No. 15-1063 (and consolidated cases)

IN THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

UNITED STATES TELECOM ASSOCIATION, *et al.*,

Petitioners,

v.

FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA,

Respondents.

ON PETITIONS FOR REVIEW OF AN ORDER OF THE FEDERAL COMMUNICATIONS COMMISSION

BRIEF FOR RICHARD BENNETT IN SUPPORT OF PETITIONERS UNITED STATES TELECOM ASSOCIATION, NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION, CTIA – THE WIRELESS ASSOCIATION, AT&T INC., AMERICAN CABLE ASSOCIATION, CENTURYLINK, WIRELESS INTERNET SERVICE PROVIDERS ASSOCIATION, ALAMO BROADBAND INC., AND DANIEL BERNINGER

David A. Balto
Counsel of Record
Matthew C. Lane
LAW OFFICES OF DAVID A. BALTO
1325 G Street, N.W., Suite 500
Washington, DC 20005
(202) 577-5424
david.balto@dcantitrustlaw.com

Attorneys for Richard Bennett

August 6, 2015

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

A. Parties

Except for the following, parties, intervenors, and amici appearing in this Court and before the FCC are listed in the Joint Brief for Petitioners United States Telecom Association, CTIA – The Wireless Association®, American Cable Association, Wireless Internet Service Providers Association, AT&T Inc., and CenturyLink:

Business Roundtable
Chamber of Commerce of the United States of America
Christopher Seung-gil Yoo
Georgetown Center for Business and Public Policy and Thirteen Prominent Economists and Scholars
Harold Furchtgott-Roth
International Center for Law and Economics Affiliated Scholars
Multicultural Media, Telecom and Internet Council
Richard Bennett
Washington Legal Foundation
William J. Kirsch

B. Ruling Under Review

The ruling under review is the FCC's Report and Order on Remand, Declaratory Ruling, and Order, *Protecting and Promoting the Open Internet*, 30 FCC Rcd 5601 (2015) ("*Order*") (JA__).

C. Related Cases

The Order has not previously been the subject of a petition for review by this Court or any other court. All petitions for review of the Order have been

consolidated in this Court, and Richard Bennett is unaware of any other related cases pending before this Court or any other court.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and D.C. Circuit Rule 26.1, the undersigned certifies that Richard Bennett is an individual and not a publicly held corporation.

By: /s/ David Balto
Attorney for Amici Curiae

CERTIFICATE OF COUNSEL REGARDING NECESSITY OF SEPARATE AMICUS CURIAE BRIEF

Pursuant to D.C. Cir. R. 29(d), Richard Bennett hereby certifies that he is submitting a separate brief from the other *amici* in this case due to the specialized nature of Richard Bennett's distinct interests and expertise. To its knowledge, Richard Bennett is the only amicus focusing on issues involving the architecture and operation of the Internet. Richard Bennett's technical knowledge of the workings of the Internet will provide a unique perspective to the court that is not shared by any other amici that we are aware of.

Richard Bennett filed a Motion for Leave to File a Separate Brief as Amicus Curiae in Support of Petitioners on July 14, 2015, see D.C. Cir. R. 29(b), which was granted August 4, 2015.

Accordingly, Richard Bennett, through counsel, certifies that filing a joint brief would not be practicable.

/s/ David Balto
David Balto

August 6, 2015

TABLE OF CONTENTS

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES…..…i

CORPORATE DISCLOSURE STATEMENT…….iii

CERTIFICATE OF COUNSEL REGARDING NECESSITY OF SEPARATE AMICUS CURIAE BRIEF……..…...iv

TABLE OF CONTENTS……..……..v

TABLE OF AUTHORITIES……..……vii

GLOSSARY……...…viii

INTEREST OF AMICI CURIAE ……..……1

INTRODUCTION AND SUMMARY OF ARGUMENT……..…...2

ARGUMENT……..…4

I. Information Services Interconnect the Networks that Comprise the Internet……....4

II. Providing Broadband Internet Access Services Depends on Information Services for their Function, Utility and Security……..5

A. Mediating the Use of Internet Bandwidth is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function…….5

B. Attack Mitigation is Necessary to Providing Broadband Internet Access Services and Requires Information Services to Function……..…….8

C. Domain Name Service is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function.....10

D. Routing is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function.……11

III. The Reclassification of Broadband Internet Access Service as a Telecommunications Service Will Impair the Internet's Ability to Support Innovation…….14

CONCLUSION……..….17

CERTIFICATE OF COMPLIANCE…….....18

CERTIFICATE OF SERVICE……...19

TABLE OF AUTHORITIES

Statutes

47 U.S.C. § 153……*passim*

Other Authorities

Filing by Richard Bennett into FCC Docket 14-28 (Dec. 30, 2014)……13

Fred Donovan, *DNS Infrastructure Is 'Highly Vulnerable' to Attacks, Warns Infonetics*, FIERCE IT SECURITY (Nov. 14, 2014)……...10

J. Postel, RFC 795 – *Service Mappings*, THE INTERNET ENGINEERING TASK FORCE (Sept. 1981)……4

Next Generation Mobile Network Alliance, *Next Generation Mobile Networks: Beyond HSPA & EVDO*, December 2006……..16

Random Early Detection, WIKIPEDIA (last visited July 27, 2015)……..7

S. Blake et al, RFC 2475 – *An Architecture for Differentiated Services*, THE INTERNET ENGINEERING TASK FORCE (December 1998) ……15

SNMP Reflected Amplification DDoS Attack Mitigation, BROADBAND INTERNET TECHNICAL ADVISORY GROUP (Aug. 2012)……11

Van Jacobson, *Congestion Avoidance and Control*, 25 COMPUTER COMM. REV. 157 (1995)……...6

GLOSSARY

3GPP	Third Generation Partnership Project, the global standards-setting body that governs mobile broadband networks
The Act	The Communications Act of 1934
ARPANET	The Advanced Research Projects Agency Network, the first large-scale experiment in packet-switching, the Internet's foundation technology.
BIAS	Broadband Internet Access Service; the FCC Order's neologism for the service provided by Internet Service Providers to the general public
DNS	Domain Name Service; the function that translates Internet domains such as google.com to numerical Internet Protocol addresses
FCC Order	FCC's Report and Order on Remand, Declaratory Ruling, and Order, Protecting and Promoting the Open Internet, 30 FCC Rcd 5601 (2015) ("Order") (JA__).
IP	Internet Protocol; the technical function that allows information to cross network boundaries. IPv4 and IPv6 refer to different versions of Internet Protocol.
ISP	Internet Service Provider; a firm that joins customer networks to the Internet as a whole
PRNET	The Bay Area Packet Radio Network, an experimental wireless packet-switching network
PSTN	Public Switched Telephone Network; the subject of Title II
SATNET	The North Atlantic Packet Satellite Network, an experimental network connecting the United States with the United Kingdom.

INTEREST OF *AMICI CURIAE*[1]

Richard Bennett is a 35-year veteran of network technology, standards, and product development with a vested interest in the Internet's continued progress. His career spans:

- Development of the modern Ethernet architecture as vice-chairman of the IEEE 802.3 1BASE5 (StarLAN) task force that devised the foundational hub-and-spoke Ethernet standard;
- Co-development of the initial Wi-Fi system architecture and inter-access point routing protocols, and subsequent co-development of the now-mandatory Wi-Fi frame aggregation scheme;
- Extensive contributions to Open System Interconnection and Internet protocols;
- Development of leading-edge Local Area Network and Internet routing devices and systems.

Richard Bennett has previously offered comments in the "Preserving the Open Internet" and "Broadband Industry Practices" dockets, GN 09-191 and WC 07-52 respectively, and offered testimony at the FCC En Banc Public Hearing on

[1] Pursuant to FRAP 29(c)(5), *amici curiae* state that no party's counsel has authored this brief either in whole or in part; that no party or its counsel contributed money that was intended to fund preparing or submitting the brief; and that no person other than these *amici curiae* and their counsel have contributed money intended to fund preparing or submitting the brief

Broadband Network Management Practices in Cambridge on February 25, 2008 as an invited technical expert.

Richard Bennett filed a Motion for Leave to File a Brief as Amicus Curiae in Support of Petitioners on July 14, 2015, see D.C. Cir. R. 29(b), which was granted August 4, 2015.

INTRODUCTION AND SUMMARY OF ARGUMENT

The FCC's reclassification of Broadband Internet Access Service (BIAS) under Title II fails to recognize both the nature of the Internet's structure and functions, and the relationship of its structure and functions to the structure and functions described in the Communications Act of 1934 (the Act). The Act defines three physical networks that it governs – the Public Switched Telephone Network (PSTN), the cable television network, and the cellular voice network – as well as a network-independent Information Service. The only rational regulatory category for BIAS in the Act's taxonomy is in the Information Service category.

In order to understand why reclassifying BIAS as a Title II telecommunications service is contrary to the functioning of the Internet, one needs to understand what the Internet is and how it functions. The Internet is a "network of networks," a virtual network or meta-network substantially independent of the many physical networks that carry Internet Protocol (IP) information packets. Functionally, each of the physical networks regulated by the Act performs a

transmission function between an end user's device or network and one or more destinations of the user's choosing. Each network performs this transmission function in a somewhat idiosyncratic way, but these individualized transmission functions do not constitute a BIAS. The Internet Service Provider (ISP) does not provide BIAS until the ISP exchanges information between its customer's network and a network provided by another ISP. This inter-network exchange of information is an Information Service as defined in the Act because it provides the customer with "the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(20).

Historically, the Internet's primary applications have been file transfer applications known to engineers as "elastic" applications because they don't have strict time-of-delivery requirements for individual information packets. This stands in sharp contrast to the PSTN subject to Title II, a network in which each unit of information is strictly time-bound. In fact, one of the Internet's significant engineering challenges is developing the mechanisms and practices that would permit it to serve non-elastic, "real-time" applications as well as or better than the PSTN does. The FCC's reclassification of BIAS thus ignores the engineering challenges of creating a world-wide network that serves both elastic and non-elastic applications at a level of quality consumers have come to expect. The

FCC's mistaken reclassification of BIAS as a Title II telecommunications service – along with the FCC's concomitant banning of broad classes of traffic management practices and services[2] – will actually impair the Internet's ability to meet the needs of diverse applications.

ARGUMENT

I. Information Services Interconnect the Networks that Comprise the Internet

By design, the Internet is a "network of networks" whose primary function is interconnection. The initial Internet consisted of three actual, tangible, physical networks: ARPANET, SATNET, PRNET. Each network provided services within its own scope and was capable of operating independently. *See* J. Postel, RFC 795 – *Service Mappings*, THE INTERNET ENGINEERING TASK FORCE (Sept. 1981), https://tools.ietf.org/html/rfc795.

The Internet allowed these separate and distinct networks to interconnect with each other, which enabled, for example, a PRNET device to communicate with a device operating on SATNET through ARPANET. The principal design elements of the Internet are a packet routing function known as Internet Protocol (IP); an end-to-end error detection, correction and pacing system known as Transmission Control Protocol; a pool of globally unique addresses (in two incompatible formats); a pool of non-unique, non-routable private addresses; and a

[2] For example, "paid prioritization" is probably critical to real-time services.

collection of non-uniform but generally interoperable algorithms and applications that are ongoing research subjects. These additional algorithms use information processing to determine and deliver bespoke transmission services, among others.

The engineering elements that join the many physical networks into a single virtual network are routers. Routers are not themselves networks and the services they perform are not simple transmission services as understood by the Communications Act; rather routers use Information Services to serve their core purpose, which is to create a single virtual network out of a plurality of diverse, physical networks by "generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(20).

Hence, the term "Internet" has never been properly understood to mean a single, tangible network in the way that the country's PSTN is. Rather, the Internet is a federation of networks that offer bespoke service levels and which interconnect with one another. "Internet" is an abbreviation of "inter-networking".

II. Providing Broadband Internet Access Services Depends on Information Services for their Function, Utility and Security

A. Mediating the Use of Internet Bandwidth is Necessary to Provide Broadband Internet Access Service and Requires Information Services to Function

As a member of the Internet, customer premise equipment is obligated to behave in a manner consistent with Internet norms, and is required to protect itself

from dangerous activities performed by other members. One example of conforming to Internet norms is the Transmission Control Protocol Congestion Control system governed by "Jacobson's Algorithm". Van Jacobson, *Congestion Avoidance and Control*, 25 COMPUTER COMM. REV. 157 (1995).

Jacobson's Algorithm requires Internet members – known as "hosts" – to reduce their rate of transmission when signaled by an Internet router that congestion is growing to dangerous levels. This signal is typically provided by the router discarding a packet.

While hosts that do not conform to Jacobson's Algorithm are not excluded from the Internet, successful operation of the Internet depends on broad conformance because normal Internet operation involves hosts cycling between underload and near overload. The Internet is thus very different from the simple telecommunications network contemplated by Title II of the Communications Act because it places the responsibility for bandwidth conservation primarily in the hands of users rather than service providers. Hosts are owned and maintained by end users, and routers are owned and maintained by ISPs; residential-focused, business-focused, and transit-focused ISPs all participate in this system, but they don't necessarily signal congestion by the same means or at the same time. The use of packet discard as a congestion signal is obviously ambiguous, because packet

discard also takes place for other reasons.[3]

Routers also implement a number of different sub-algorithms of the Jacobson master scheme, such as Random Early Detection, Weighted Random Early Detection, and several other means. *See Random Early Detection*, WIKIPEDIA, http://en.wikipedia.org/wiki/Random_early_detection (last visited July 27, 2015). The choice and execution of these algorithms is an example of close interaction between customer premise equipment and ISPs, not only those that directly serve the end user but also those connected to other ISPs that are connected to the end user's ISP.

Implementing Jacobson's Algorithm requires extensive information processing in both the customer's host and the ISP's router, in part to distinguish packet loss due to congestion from that caused by other factors, and in part to select and implement the most effective mechanism for bandwidth mediation.

There is no function in telecommunications services that compares to the dynamic interaction that occurs between ISPs and their customers to mediate access to bandwidth. To the contrary, the PSTN typically connects calls between parties on the same network. When a telephone customer places a call on the PSTN, he or she signals a destination and the network either puts the call through or denies it. If the call is connected, each user has exclusive access to a fixed

[3] For example, when wireless packets collide, they tend to be dropped by the receiving host because their information content can't be trusted.

bucket of communications bandwidth for the duration of the call, regardless of the nature of the caller's wishes or of other activities taking place on the network at the same time.

BIAS operates in a radically different way. BIAS provides neither a strict bandwidth limit for each connection nor a guarantee that any user or service will control the path to any other user or service. BIAS provides an opportunity to communicate and a flexible outcome, but telecommunications service ensures a limited outcome in a limited domain.

This is in accord with the fact that the Internet is a statistical system that delivers services by estimating its finite resources, assessing the desires of end user applications, and arriving at a series of dynamic compromises that apportion resources to applications. This is an information processing exercise. Telecommunications services regulated under Title II of the Act do not perform this function but BIAS does.

B. Attack Mitigation is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function

Billions of people use the Internet through their own computers worldwide, and (unsurprisingly) some are up to no good. The connectionless nature of Internet Protocol makes it an ideal vehicle for denial of service attacks. The insecure nature of basic Domain Name Service (DNS) allows criminals to use DNS as an amplifier

for attacks. Further, distributed denial of service attacks are made possible by viruses that enable botnet operators to invade and take over end-user systems in order to enlist them into their botnets, where they can be used to send spam and take part in distributed denial of service attacks. Mitigating these attacks requires ISPs to engage a multi-pronged strategy, using information technology to distribute anti-virus software to end user computers, to monitor networks for suspicious traffic and attacks, to block (or redirect) attack traffic when it is found, and to notify other ISPs of infected computers on the other ISP's network.

Attack mitigation is not simply a management function performed to make networks operate better. Rather, it is an essential service that is necessary to ensure the integrity of customer equipment. The most obvious and well-known element of attack mitigation is the anti-virus software that ISPs make available to their customers, typically free of charge. Anti-virus software is an intensive use of information processing to search for viruses in downloads and incoming email, to monitor the integrity of system files, and to distribute attack knowledge to software producers.

Attack mitigation capabilities are critical to the provision of safe and secure BIAS. Absent attack mitigation capabilities, which rely on Information Services to function, BIAS could never be provided in a safe or secure manner. Further, such capabilities are Information Services as defined in the Act because they include

"the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(20).

C. Domain Name Service is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function

BIAS always includes DNS provided over "the largest distributed database in the world." Fred Donovan, *DNS Infrastructure Is 'Highly Vulnerable' to Attacks, Warns Infonetics*, FIERCE IT SECURITY (Nov. 14, 2014), http://www.fierceitsecurity.com/story/dns-infrastructure-highly-vulnerable-attacks-warns-infonetics/2014-11-13. DNS is an increasingly sophisticated distributed function that translates domain names into Internet protocol addresses. In addition, DNS implements the Domain Name System Security Extensions[4] protocol, an authentication service that validates the correctness of the domain name and maps it to an to Internet Protocol address thereby protecting users from security attacks, especially "man in the middle" attacks in which a bad actor impersonates the service requested by the user. DNS is also a traffic direction service that connects Content Delivery Network users to the nearest and/or fastest location.

DNS manages aliased domain names – multiple domain names sharing a common IP address – and provides both IPv4 and IPv6 addresses. DNS

[4] Commonly referred to as DNSSEC.

distinguishes multiple services within a domain, such as the email "Mail Exchanger" and the web service. The database managed by a DNS server is updated in real time, with updates shared across the entire Internet as needed. Further, DNS servers protect themselves from attacks, since a simple, unprotected DNS server is an attack vector that can amplify distributed denial of service attacks. See *SNMP Reflected Amplification DDoS Attack Mitigation*, BROADBAND INTERNET TECHNICAL ADVISORY GROUP (Aug. 2012), http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

DNS may be provided by third parties, but the typical user of BIAS uses the DNS provided by his or her ISP. Without ISP-provided DNS, it would be impossible for the typical user to even connect to a third party DNS in the first instance. Therefore, DNS is much more complex than mere "capability for the management, control, or operation of a telecommunications system," but is actually integral to the provision of BIAS. 47 U.S.C. § 153(24).

D. Routing is Necessary to Providing Broadband Internet Access Service and Requires Information Services to Function

Routing is an indispensable element of any packet-switched network such as the Internet. In its most elementary form, routing functions determine whether packets of information received by a router are to be dropped, forwarded, or processed.

A packet is dropped if it comes from an unauthorized source, or if the forwarding path is congested or unavailable. A packet is forwarded if its network identifier matches a known valid route and resources are available for forwarding. Packets are processed if they contain management information such as routing map updates, network management commands, or service specifications.

In commercial settings, all packets potentially have implications for accounting, security, and public safety, so routers also provide these functions. Network Quality of Service is provided and ensured by routers, and these functions are present in routers in a number of different forms.

This architecture is quite different from the way the PSTN is designed and operates. The telephone network determines a path from the calling to the called party when calls are set up. It simply records a circuit identifier at the time a call is established, which is used by all subsequent elements of the call. Packet switching routers, on the other hand, recalculate the route from source to destination every time a packet is forwarded, a much more intensive information-processing task as compared to connecting voice calls on the PSTN. Packet routers also react to network failures by choosing alternate routes while a packet is in flight, sometimes reacting to network failures in small fractions of a second. Consequently, packet routers perform several orders of magnitude more computation than telephone network switches do.

It is useful to compare the functions performed by common web servers with those performed by Internet routers. There is no dispute that web services are Information Services, so it follows that ISP services performed over routers must be information services as well if the two are essentially similar or if routers are more information service intensive.

In a filing with the FCC in the matter of the FCC Order, Richard Bennett provided a chart comparing the functions of web servers and routers according to the specific terms of the Act's definition of Information Service ("the capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications." 47 U.S.C. § 153(20). *See* Filing by Richard Bennett in FCC Docket 14-28 at 10 (Dec. 30, 2014), *available at* http://apps.fcc.gov/ecfs/document/view?id=60001011505.

In nearly every case, the functions performed by the router are more information processing-intensive than the corresponding web server functions. Because the Internet is a highly complex information system, routers perform significantly more information processing than web servers and similar functions attached to the Internet.

The Internet routing function is more information processing-intensive than Telecommunications Service call processing, and it requires a degree of flexibility

foreclosed by the FCC Order's insistence that routing be performed without regard for application requirements or short-lived network conditions.

III. The Reclassification of Broadband Internet Access Service as a Telecommunications Service Will Impair the Internet's Ability to Support Innovation

BIAS is a highly specialized information technology-enabled service that can only be provided by highly skilled operators with a deep pool of talent and a major investment in equipment, training, and infrastructure. It makes no more sense to classify BIAS as a simple telecommunication service than it would to classify integrated circuit design and production as a telecommunication service simply because some chips are used in telephone networks. These are two vastly different realms, and to confuse them is to commit an egregious error, not just for regulating the Internet, but also for the ability of engineers to successfully manage and design Internet operations going forward.

The FCC's record in this proceeding is replete with technically and economically sound descriptions of the Internet's architecture and operation. These filings make it clear that BIAS is much more than simple transmission. Rather than giving these filings due weight, the Commission's Order brushed them aside in favor of simplistic analyses offered by self-interested advocates with no technical expertise.

At a bare minimum, the FCC should have acknowledged the reasoned

analysis of skilled technologists and provided reasons for taking the path it took. But the FCC Order failed to acknowledge the filings of network engineers, professors of network science and engineering, router manufacturers, and network operators that offered the agency clear evidence that the Internet is not organized and operated as the Agency represents. Because the Internet is radically different from the FCC Order's version of the Internet, the FCC's reclassification of BIAS and attendant regulations are directly at odds with the current and future utility of the Internet for ordinary citizens and innovators alike.

For example, the FCC's use of Title II as a pretext for imposing a uniform service model on BIAS (no throttling, no paid prioritization) prevents providers from offering services described in RFC 2475,[5] which says: "[s]ervice differentiation is desired to accommodate heterogeneous application requirements and user expectations, and to permit differentiated pricing of Internet service." S. Blake et al, RFC 2475 – *An Architecture for Differentiated Services*, THE INTERNET ENGINEERING TASK FORCE (December 1998) https://tools.ietf.org/html/rfc2475, page 3. RFC 2475 is an Informational RFC rather than an Internet Standard, but the architecture it describes has become the basis for Differentiated Services widely deployed across the Internet.

[5] RFCs are publications of the Internet Engineering Task Force and the Internet Society and function as *de facto* Internet standards. RFC is no longer considered to be an acronym.

Similarly, the FCC Order's uniform service model conflicts with the use of Integrated Services in Third Generation Partnership Project (3GPP) mobile networks to support Voice over LTE. 3GPP has determined that the voice application requires the use of Integrated Services to function over IP. See Next Generation Mobile Network Alliance, *Next Generation Mobile Networks: Beyond HSPA & EVDO*, December 2006, http://ngmn.org/uploads/media/Next_Generation_Mobile_Networks_Beyond_HSPA_EVDO_web.pdf.

The FCC Order means BIAS providers can no longer sell access to the Internet's entire set of standards; in effect, it makes the FCC the arbiter of Internet architecture, a function that has always been played by the Internet Engineering Task Force in the past.

The FCC Order has closed the Internet to applications and services that require specialized treatment. Consequently, the FCC Order impairs the operation of the Internet and prevents it from meeting the needs of innovators and the general public in the future as its designers intended and its users require.

CONCLUSION

I urge the Court to vacate the FCC's misclassification of Broadband Internet Access Service. The FCC has erred, and the error must be corrected lest the future of the Internet is compromised.

Respectfully submitted,

/S/ David A. Balto
David A. Balto
Counsel of Record
Matthew C. Lane
Law Offices of David A. Balto
1325 G Street, N.W., Suite 500
Washington, DC 20005
(202) 577-5424
david.balto@dcantitrustlaw.com

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 3,394 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Word 2013 in 14-point Times New Roman font.

Dated: August 6, 2015

By: /s/ David Balto
Attorney for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system on August 6, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

By: /s/ David Balto
Attorney for Amici Curiae