ORAL ARGUMENT SCHEDULED FOR 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 Petition for Review from the Federal Communications Commission

---

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND THE AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL IN SUPPORT OF THE RESPONDENTS

LEE ROWLAND
SAMIA HOSSAIN
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, NY 10004
Tel: (212) 549-2550
Email:lrowland@aclu.org

ARTHUR B. SPITZER
AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL
4301 Connecticut Ave.
Washington, D.C. 20008
Tel: (202) 457-0800
Email: artspitzer@aclu-nca.org

CORYNNE MCSHERRY
KIT WALSH
LEE TIEN
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Facsimile: (415) 436-9993
Email: corynne@eff.org

September 21, 2015

Counsel for Amici Curiae

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rules 26.1 and 28(a)(1), and Fed. R. App. P. 26.1, the undersigned counsel certifies as follows:

A. Parties and *Amici* Except for the following *amici*, all parties and intervenors appearing before the FCC and this Court are listed in the Joint Brief for Petitioners United States Telecom Association *et al*. In this Court, the following amici have been granted leave to participate:

- Harold Furchtgott-Roth
- Internet Association
- Washington Legal Foundation
- Consumers Union
- Competitive Enterprise Institute
- American Library Association
- Richard Bennett
- Association of College and Research Libraries
- Business Roundtable
- Association of Research Libraries
- Center for Boundless Innovation in Technology
- Officers of State Library Agencies
- Chamber of Commerce of the United States of America

- Open Internet Civil Rights Coalition
- Georgetown Center for Business and Public Policy
- International Center for Law and Economics and Affiliated Scholars
- William J. Kirsch
- Computer & Communications Industry Association
- Mobil Future
- Mozilla
- Multicultural Media, Telecom and Internet Council
- Engine Advocacy
- National Association of Manufacturers
- Phoenix Center for Advanced Legal and Economic Public Policy Studies
- Dwolla, Inc.
- Telecommunications Industry Association
- Our Film Festival, Inc.
- Christopher Seung-gil Yoo
- Foursquare Labs, Inc.
- General Assembly Space, Inc.
- Github, Inc.
- Imgur, Inc.

- Keen Labs, Inc.
- Mapbox, Inc.
- Shapeways, Inc.
- Automattic, Inc.
- A Medium Corporation
- Reddit, Inc.
- Squarespace, Inc.
- Twitter, Inc.
- Yelp, Inc.
- Media Alliance
- Broadband Institute of California
- Broadband Regulatory Clinic
- Tim Wu
- Edward J. Markey
- Anna Eshoo
- Professors of Administrative Law
- David T. Goldberg
- Joseph Carl Cecere, Jr.

B. Rulings 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 F.C.C. Rcd. 5601 (2015) ("Order") [JA___].

C. Related Cases

There are no other cases related to the consolidated petitions.

September 21, 2015

/s/ Corynne McSherry
Corynne McSherry

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rule 26.1 and Federal Rule of Appellate Procedure 26.1, *amici* submit the following corporate disclosure statement:

Amicus Electronic Frontier Foundation ("EFF") is a donor-funded, non-profit civil liberties organization. EFF has no parent corporation, and does not issue stock.

Amici American Civil Liberties Union ("ACLU") and American Civil Liberties Union of the Nation's Capital are privately-funded, non-profit civil liberties organizations. The ACLU and ACLU of the Nation's Capital have no parent corporation, and do not issue stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES*

Cases

*Authorities upon which we chiefly rely are marked with asterisks.

Administrative Rulings

Other Authorities

GLOSSARY

AA: Application Agnosticism. The Order defines an application-agnostic practice as one that either "does not differentiate in treatment of traffic, or . . . differentiates in the treatment of traffic without reference to content, application or device."[1]

BIAS: Broadband Internet Access Service. The Order defines BIAS as:

> *A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part.*[2]

FCC: Federal Communications Commission.

ISP: Internet Service Provider. As used in this brief, the term generally refers to Broadband Internet Service Providers.

[1] Order ¶ 144 n.344.

[2] *Id.* ¶ 25.

INTEREST OF AMICI[3]

EFF is a member-supported nonprofit organization devoted to protecting civil liberties and free expression in technology, law, policy, and standards. With over 27,000 dues-paying members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment. EFF has campaigned both in the United States and abroad against ill-considered efforts to block, filter, or degrade access to the public Internet. EFF develops and promotes tools that help consumers and public interest groups test their broadband connections to see if their providers are interfering with the traffic to and from users' computers. EFF was among the first to independently test and discover the nature and scope of Comcast's 2007 interference with BitTorrent and other peer-to-peer applications.

The ACLU is a nationwide, nonprofit, nonpartisan organization with approximately 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Founded in 1920, the ACLU has vigorously defended the First Amendment in state and federal courts across the country. *See, e.g.*, *Reno v. ACLU*, 521 U.S. 844 (1997). The ACLU has also been at the forefront of efforts to ensure that the Internet remains a

[3] No party's counsel authored this brief in whole or in part. No party or party's counsel, nor any person besides *amici*, their members, or their counsel contributed money toward this brief.

free and open forum for the exchange of information and ideas. The ACLU has served as counsel and *amicus* in several cases involving online speech. For years, the ACLU has advocated for net neutrality through legislative advocacy and public education efforts. The American Civil Liberties Union of the Nation's Capital is the Washington, D.C., affiliate of the National ACLU.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Net neutrality is one of the most important free speech issues of the digital age. Fair access to high-quality Internet is essential to our ability to retrieve and share information, which in turn enables us to shape our political, civic, and social discourse. Internet Service Providers ("ISPs") hold the key to this world of information. Absent effective neutrality rules, ISPs can—and some undoubtedly will—act as gatekeepers to digital information, rather than neutral conduits for speech. Content providers will have their online speech throttled and censored. The Open Internet Order sets forth rules that are necessary to prevent such discrimination and protect this free marketplace. Ultimately, the Order advances a core purpose of the First Amendment: "to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail, rather than to countenance monopolization of that market." *Red Lion Broad. Co. v. FCC*, 395 U.S. 367, 390 (1969).

According to the World Bank, nearly 90% of Americans use the Internet.[4] It has become essential to our democracy—for example, by providing real-time engagement with government,[5] a forum for anonymous criticism,[6] and a source of independent journalistic perspectives.[7] The Internet is an important tool for innovators to test out new ideas, reach untapped markets, and build on one another's designs.[8] The significance of individuals' First Amendment interests in accessing information from an uncensored Internet can hardly be overstated.

Upstart blogs, innovative media, libraries, and non-profits are all unlikely to be able to negotiate with ISPs for "fast lane" arrangements that, without the Order, will be available to others.[9] Because the Internet service market is dysfunctional,

---

4 Internet Users (Per 100 People), World Bank, http://data.worldbank.org/indicator/IT.NET.USER.P2 (last visited Sept. 17, 2015).

5 See, e.g., @WhiteHouse, Twitter, https://twitter.com/whitehouse; U.S. Dep't of State, Alerts and Warnings, http://travel.state.gov/content/passports/english/alertswarnings.html (last visited Sept. 17, 2015).

6 See James A. Gardner, *Anonymity and Democratic Citizenship*, 19 Wm. & Mary Bill Rts. J. 927 (2011).

7 See, e.g., Damien Cave & Rochelle Oliver, *The Videos That Are Putting Race and Policing Into Sharp Relief*, N.Y. Times (Aug. 12, 2015), http://www.nytimes.com/interactive/2015/07/30/us/police-videos-race.html?_r=0.

8 See Julius Genachowski, Chairman, FCC, Remarks at the Joint Center for Political and Economic Studies: Media & Technology Policy Forum (Mar. 3, 2010), available at https://www.fcc.gov/events/speech-open-internet-innovation-and-economic-development ("Internet openness is key to a healthy business ecosystem, particularly for startups and small businesses, which are America's engine of growth and opportunity.").

9 *Id.*

market forces cannot prevent or remedy such discriminatory practices. Against this background, carefully tailored regulation is appropriate and necessary to protect the vibrant marketplace of online speech.

The FCC's Order sets out appropriate rules to vindicate those interests. The Order classifies Broadband Internet Access Service ("BIAS") Providers as common carriers under Title II of the Communications Act, and subjects them to simple rules to ensure that ISPs remain neutral conduits of speech. The Order establishes three bright-line rules for BIAS: (i) no blocking of access to legal content, (ii) no throttling (slowing) of lawful Internet traffic on the basis of content, and (iii) no paid prioritization of traffic in exchange for consideration or benefit to an affiliated entity.[10] Essentially, the Order requires ISPs to behave as they traditionally have: delivering digital speech without undue interference or censorship.

This regulation merits, and meets, constitutional scrutiny. BIAS is largely provided via two methods: cable wires and wireless radio spectrum. Both infrastructures are already regulated as common carriers—with the Supreme Court's blessing. To preserve access to the 21st Century's marketplace of ideas,

[10] *See* Order ¶¶ 14-19. In addition to the bright-line rules, the Order includes a "general conduct" rule explaining that the overall purpose of the Order is to avoid harm to consumers and content providers. Order ¶ 21. As set forth in Section III, *infra*, amici file this brief to defend the bright-line rules and explain how the general conduct rule can be properly construed to further these rules.

ISPs may be similarly regulated. Because ISPs function as conduits and are not in the business of endorsing the speech they deliver, the Order's impact on expression is minimal. And because they operate as conduits over scarce infrastructure subsidized and provided by government, Supreme Court precedent supports its constitutionality.

The Order strikes the correct balance in protecting the enormous individual speech interests at stake from the power of ISPs to play gatekeeper to the online world.

ARGUMENT

I. The Open Internet Is Essential to Speech and Innovation.

A. The Internet Was Built on Principles of Neutrality.

The Internet grew into a powerhouse platform for free expression because of legal and technological conditions that prevented content discrimination by ISP networks.

The Internet consists of tens of thousands of individual networks of computers and other devices, owned, operated, and maintained by different entities.[11] To facilitate global communication, each network interconnects to one or more other networks, thus the term "Internet." While each network speaks the

[11] *CIDR Report for 17 Sep 15*, CIDR REPORT, http://www.cidr-report.org/as2.0/ (last visited Sept. 17, 2015).

same language ("protocol"), the networks vary widely in their architecture and their underlying technology. A typical ISP network connects anywhere from dozens to thousands of homes and businesses or mobile devices to the rest of the Internet.[12]

In the early 1990s, when the Internet became a mass communications medium, most Internet access operated through dial-up connections. Customers accessed the Internet by connecting directly to ISPs over telephone lines. Dial-up encouraged free-market competition; individuals could choose which ISP to use, and then connect directly to that company. If they didn't like their ISP, they could connect to a new provider simply by dialing a different phone number. This spurred development of a healthy and competitive ISP marketplace, with thousands of providers offering Internet access across the United States.[13]

---

[12] The same company may act in different roles: a large ISP can provide service to other ISPs, or a large consumer-facing provider may own core infrastructure. Thus, it is important to focus on the context in which ISPs are being discussed, or risk confusion and imprecision. *See generally* Joint Statement of Internet Engineers 3 & n.4, *available at* https://www.eff.org/files/2015/09/14/eff-aclu_internet_engineers_and_pioneers_statement.pdf, attached hereto as Appendix A.

[13] Jason Oxman, *The FCC and the Unregulation of the Internet* 17 (FCC Office of Plans and Policy, Working Paper No. 31, July 1999), *available at* https://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.doc at 15 ("Over 6,000 Internet service providers (ISPs) today offer dial-up service to the Internet, and over 95% of Americans have access to at least four local ISPs.").

That competition was fostered at the "last mile"—that is, the point of delivery to individual consumers—by existing common carrier rules and other FCC regulations that curbed the power of telephone companies. For example:

- In 1975, the FCC prohibited telephone companies from blocking their customers from attaching their own equipment to the phone network. If not for this ruling, AT&T could have blocked the use of dial-up modems.[14]

- In 1980, the FCC required telephone companies to offer "data services" through separate affiliates because they would otherwise have had both the ability and the incentive to use their control of the telephone network to discriminate against unaffiliated, competing data services.[15]

- In 1983, the FCC prevented telephone companies from charging ISPs by the minute for their use of the local telephone network. Had the Commission allowed such charges, consumers would have paid per-minute fees for Internet access. That would have slowed Internet growth, as such fees did in Europe.[16]

Though common carriage regulations helped foster the emerging Internet, by the early 2000s, Americans were increasingly replacing dial-up connections with broadband. Technologically, wired broadband service has been provided through the coaxial cables used by cable television companies, fiber-optic cables, or digital subscriber line ("DSL") connections that achieve high speeds over regular telephone wires with limited geographic range. These connections are subject to

[14] *See* Proposals for New or Revised Classes of Interstate and Foreign Message Tolls Telephone Service (MTS) and Wide Area Telephone Service (WATS), 56 F.C.C.2d 593 (1975).

[15] Amendment of Section 64.702 of the Commission 's Rules and Regulations (Second Computer Inquiry), 77 F.C.C.2d 384 (1980).

[16] *See* MTS and WATS Market Structure, 97 F.C.C.2d 682 (1983).

more centralized control than dial-up connections. Customers can no longer simply dial into a preferred ISP located anywhere on the telephone network; they are tethered to ISPs operating over *local* phone or cable lines. As a result, the growth of broadband means an ever-smaller number of companies delivering access to an ever-larger slice of the population.

The level of service ("bandwidth") a broadband subscriber receives for communicating information has not typically been altered by ISPs based on content. Customers normally pay for a certain amount of bandwidth (for example, 25 megabits per second). Sometimes a plan involves a "data cap": a limit on how much data the customer can move across the company's system. Different plans let customers pay for more bandwidth or a higher data cap. Historically, data caps have generally been neutral as to how customers use their data allowance.[17] This informal system of network neutrality has resulted in part from anti-monopoly rules attached to several of the largest broadband provider mergers.[18]

This structure has enabled an explosion of innovation over the past 25 years. Google, for instance, started as two students with a better search algorithm. If they had needed to negotiate deals with Comcast, Verizon, and other

[17] *See* Erik Sherman, *What will a non-neutral Internet really be like?*, MONEYWATCH (Jan. 15, 2014), http://www.cbsnews.com/news/what-will-a-non-neutral-net-really-be-like/.

[18] *See, e.g.*, Final Judgment at 9-32, *United States v. Comcast Corp*. (Sept. 1, 2011) (No. 05-1631), 2011 WL 5402137, at *4-16.

telecommunications companies, they might never have overcome the incumbent search giants of the time: Excite and Alta Vista. The same holds true for many other innovators, including marketplaces like eBay, Amazon, and Etsy, and social media platforms like Facebook and Twitter. They have thrived in large part because neither service providers nor anyone else had an advance economic veto right on new applications, services, or content.

In short, the Internet has become so successful and so central to our lives *because* it was built on neutrality principles.

B. The Internet Is Now the Core Platform for Free Speech and Access to Knowledge.

Today, the Internet has become our public square, our newspaper, our megaphone, and more. The Supreme Court rightly called the Internet "the most participatory form of mass speech yet developed." *Reno*, 521 U.S. at 863. The Internet has led to new forms of political activism,[19] news-gathering,[20] and speech access and distribution that do not rely on central curators.

---

[19] *See, e.g.*, Ashraf M. Attia et al., *Commentary: The Impact of Social Networking Tools on Political Change in Egypt's "Revolution 2.0,"* 10 ELECTRONIC COM. RES. & APPLICATIONS 369 (2011).

[20] Monica Anderson & Andrea Caumont, *How Social Media Is Reshaping News*, PEW RES. CTR. (Sept. 24, 2014), http://www.pewresearch.org/fact-tank/2014/09/24/how-social-media-is-reshaping-news/.

A 2012 study found that 40% of all American adults post political content to social media sites.[21] The 2010 election cycle, for example, featured citizen videos on numerous campaign topics, including immigration, health care, education and teachers' unions, the federal budget deficit, bank bailouts, and taxes.[22] Citizens have also used new technology and high-bandwidth connections to share original videos and remixes of political ads, commercials, and mass media. Examples include remixes of mass media to highlight sexism; remixes of presidential debates to demonstrate repetition of rehearsed talking points; and remixes of commercials to criticize private companies.[23]

The Internet is also a portal to education, health, and employment for people of all ages. Two-thirds of students used the Internet for homework in 2009, and those not online were at a "growing disadvantage."[24] Thanks to higher-bandwidth connections, universities offer a wide range of interactive, online education

---

[21] *See* Lee Rainie & Aaron Smith, *Social Networking Sites and Politics: Main Findings*, PEW RES. CTR. (Mar. 12, 2012), http://www.pewinternet.org/2012/03/12/main-findings-10/.

[22] *The 2010 Election on YouTube: By the Numbers*, CITIZENTUBE (Nov. 1, 2010), http://www.citizentube.com/2010/11/2010-election-on-youtube-by-numbers.html.

[23] *DIY Video 2010: Political Remix (Part Two)*, MIT CTR. FOR CIVIC MEDIA (Nov. 15, 2010), https://civic.mit.edu/blog/henry/diy-video-2010-political-remix-part-two.

[24] Fed. Commc'ns Comm'n, September Commission Meeting Presentation 7 (2009), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-293742A1.pdf.

courses.[25] The majority of Americans use the Internet to seek health information and jobs.[26] High-bandwidth connections allow video interviews for job and university applications and allow patients to connect more readily with doctors.[27]

In short, high-bandwidth channels of expression are crucial to speech, civic participation, and basic socioeconomic activity.

C. Permitting ISPs to Act as Gatekeepers Threatens Free Expression and Innovation.

Absent net neutrality rules, ISPs can effectively censor political speech, prevent competitors from reaching their customers over the Internet, and reshape the Internet so that selected and curated content stifles the free flow of education, research, and news.

The risks of allowing ISP discrimination are illustrated by incidents abroad, where neutrality norms have been less robust. ISPs discriminate against particular speakers and technologies even in jurisdictions with strong transparency requirements and significantly more competition than in the United States. Such

[25] Examples include udacity.com, coursera.com, copyX.org, and ocw.mit.edu.

[26] Fed. Commc'ns Comm'n, September Commission Meeting Presentation 7 (2009), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-293742A1.pdf.

[27] *Teleheath Use in Rural Heathcare*, RURAL ASSISTANCE CTR., https://www.raconline.org/topics/telehealth (last visited Sept. 17, 2015).

discrimination affects over 75% of subscribers in the UK[28] and at least one in five subscribers in the European Union.[29] They include restrictions on online phone services, file transfer technologies, and gaming, streaming, email, and messaging applications.[30] One Canadian ISP even blocked access to the speech of its political opponents.[31]

While less widespread, ISPs have engaged in similar practices in the United States. Several ISPs have overlaid third-party website content with their own advertisements, sometimes blocking the original content.[32] ISPs as large as

---

[28] Alissa Cooper, *How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom* (Sept. 2013) (Published Ph.D. dissertation, University of Oxford), *available at* https://www.alissacooper.com/files/Chapter6-final.pdf.

[29] Body of European Regulators for Elec. Comm., *A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe* (May 29, 2012), *available at* http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf.

[30] *Id.*

[31] *Telus Cuts Subscriber Access to Pro-union Website*, CBCNEWS CAN. (July 24, 2005), http://www.cbc.ca/news/canada/telus-cuts-subscriber-access-to-pro-union-website-1.531166.

[32] Karl Bode, *Mediacom Not Talking about Javascript Ad Injection: Users Still Waiting on an Explanation*, DSLREPORTS (Mar. 3, 2011), https://www.dslreports.com/shownews/Mediacom-Not-Talking-About-Javascript-Ad-Injection-113007; Zachary Henkel, *ISP Advertisement Injection: CMA Communications* (Mar. 29, 2013), http://zmhenkel.blogspot.com/2013/03/isp-advertisement-injection-cma.html; Jonathan Mayer, *AT&T Hotspots: Now with Advertising Injection*, WEB POLICY BLOG (Aug. 25, 2015), http://webpolicy.org/2015/08/25/att-hotspots-now-with-advertising-injection/.

AT&T[33] and as small as Madison River[34] have tried to block their subscribers from communicating with competitors. Comcast secretly interfered with lawful peer-to-peer file transfer technologies.[35] Verizon refused to allow smartphone owners to use their phones as wireless access points (ultimately reaching a $1.25 million settlement with the FCC).[36] And at least two large BIAS companies have censored political speech on their *other* platforms not subject to net neutrality rules: Verizon blocked pro-choice text messages[37] and AT&T censored criticism of George Bush during a concert webcast.[38]

---

[33] *See* David Kravets, *AT&T Holding FaceTime Hostage Is No Net-Neutrality Breach*, WIRED.COM (Aug. 22, 2012), http://www.wired.com/2012/08/facetime-net-neutrality-flap/.

[34] *See* Madison River Commc 'ns, LLC and Affiliated Companies, 20 F.C.C. Rcd. 4295 (2005).

[35] *See* Press Release, Fed. Commc'n Comm'n, Commission Orders Comcast to End Discriminatory Network Management Practices, (Aug. 1, 2008), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf.

[36] *See* Complaint of Free Press Against Cellco Partnership d/b/a Verizon Wireless for Violating Conditions Imposed on C Block of Upper 700 Mhz Spectrum (June 6, 2011), *available at* http://www.freepress.net/sites/default/files/fp-legacy/FreePress_CBlock_Complaint.pdf; Press Release, Fed. Commc'ns Comm'n, *News Release: Verizon Wireless to Pay $1.25 Million to Settle Investigation Into Blocking of Consumers ' Access to Certain Mobile Broadband Applications* (July 31, 2012), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db0731/DOC-315501A1.pdf.

[37] Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. TIMES (Sept. 27, 2007), http://www.nytimes.com/2007/09/27/us/27verizon.html.

[38] *AT&T Calls Censorship of Pearl Jam Lyrics an Error*, REUTERS (Aug. 9, 2007), http://www.reuters.com/article/technologyNews/idUSN091821320070809.

Broadband providers have also demonstrated interest in creating artificial scarcity by segmenting bandwidth into multiple markets rather than investing in neutral, general-purpose upgrades.[39]

Such artificial scarcity threatens innovation. Comcast's decision to degrade Netflix's ability to deliver information to subscribers over Comcast's network exemplifies the coercive power of ISPs. This rendered the service practically unusable.[40] When Netflix paid the toll Comcast demanded, quality was rapidly restored.[41]

Moreover, while Netflix could afford to pay for priority access for streaming video, new innovators attempting to enter the market almost certainly cannot. Etsy, Inc.—now a major e-commerce website with hundreds of millions of dollars per year in revenue—noted that it would likely have failed if it had to pay for similar

[39] Zachary M. Seaward, *The Inside Story of How Netflix Came to Pay Comcast for Internet Traffic*, QUARTZ (Aug. 27, 2014), http://qz.com/256586/the-inside-story-of-how-netflix-came-to-pay-comcast-for-internet-traffic/.

[40] *Id.*

[41] *Id.*

priority access to consumers.[42] Other small businesses and their investors have echoed these concerns.[43]

Noncommercial Internet applications are also likely to be relegated to the slow lane, or disappear altogether if they require broadband speeds to function. Across the country, people depend on high-speed Internet to access a variety of public and nonprofit services. Hospitals, libraries, firefighters, churches, schools, and social service organizations need fast Internet, but such entities may have difficulty negotiating special deals with quasi-monopolies to get it.[44]

These risks are not hypothetical. ISPs have a record of interfering with speech to serve their financial interests and censor critics, and a continuing interest

---

[42] Comments of Etsy, Inc. at 5, *Promoting the Open Internet* (July 8, 2014) (GN Docket Nos. 14-28 & 10-127), *available at* https://blog.etsy.com/news/files/2014/07/Etsy-Open-Internet-Comments-7.8.14.pdf.

[43] *See, e.g.* Comment of Open Media and Information Companies Initiative (OpenMIC), et al., *Promoting the Open Internet* (GN Docket No. 14-28) (July 14, 2014), *available at* http://openmic.org/files/Open%20MIC%20et%20al_GN%20Docket%20No.%2014-28_Comment.pdf; Letter from Open Engine & The Open Tech. Inst. at the New Am. Found., to Fed. Commc 'ns Comm'n (May 7, 2014), *available at* http://engine.is/wp-content/uploads/Company-Sign-On-Letter.pdf; Mike Masnick, Kickstarter, *Etsy and Dwolla All Speak Out On Net Neutrality and Why the FCC's Plan Is Dangerous to Innovation*, TECHDIRT (July 11, 2014), https://www.techdirt.com/articles/20140710/17450827845/kickstarter-etsy-dwolla-all-speak-out-net-neutrality-why-fccs-plan-is-dangerous-to-innovation.shtml.

[44] *See, e.g.*, Andrea Peterson, *Why the Death of Net Neutrality Would Be a Disaster for Libraries*, WASH. POST (May 16, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/16/why-the-death-of-net-neutrality-would-be-a-disaster-for-libraries/.

in doing so. Indeed, the FCC and this Court have identified several examples, *see* *Verizon v. FCC*, 740 F.3d 623, 645-46, (D.C. Cir. 2014) (citing Preserving the Open Internet, 25 F.C.C. Rcd. 17905 (2010) ("2010 Order")), including:

- Broadband Internet access providers "have incentives to interfere with the operation of third-party Internet-based services that compete with the providers' revenue generating telephone and/or pay-telephone services," *id.* at 645-46 (citing 2010 Order at 17919 ¶22).

- "[B]roadband providers' position in the market gives them the economic power to restrict edge[content]-provider traffic and charge for the services they furnish edge providers. . . . [The] provider functions as a 'terminating monopolist' . . . [and has] this ability to act as a 'gatekeeper'," *id*. at 646 (citing 2010 Order ¶ 24);

- "[E]nd users are unlikely to [switch to a competing broadband provider]" as "end users may not know" that their broadband provider is behaving in non-neutral ways and "even if they do have this information [consumers] may find it costly to switch," *id.* at 646-47 (citing 2010 Order ¶ 27);

- "[B]roadband providers' potential disruption of edge-provider traffic [is] itself the sort of 'barrier' that has 'the potential to stifle overall investment in Internet infrastructure,'" *Id.* at 642-43 (citing 2010 Open Internet Order ¶ 120);

- In light of recent history, "the threat that broadband providers would utilize their gatekeeper ability to restrict edge-provider traffic is not . . . 'merely theoretical.'" *Id.* at 648 (citing 2010 Open Internet Order ¶ 35). Clear, focused rules of the road can help ward off these threats, to the benefit of the public interest.

D. The BIAS Market Is a Dysfunctional, Government-Enabled Oligopoly.

ISPs can play a censorial role in part because each holds a unique position of centralized power over its customers. In order to reach any endpoint on the Internet

(such as a website), the customer must go through her ISP's network. The ISP has the power to downgrade or sever that link, so that its subscriber cannot reach a particular endpoint, access its content, or use a particular hardware device or software app to do so.

The ISP market was born and remains anchored on top of existing common carrier networks subsidized and provided by government. Incumbent ISPs have benefited from government assistance to defray prohibitive costs of local infrastructure construction. Federal law requires phone companies to give the cable industry access to telephone poles at preferential rates set by FCC.[45] Wireless Internet providers have benefited from physical and regulatory groundwork laid by the radio industry,[46] in which "existing broadcasters . . . attained their present position because of their initial government selection in competition with others before new technological advances opened new opportunities for further uses." *Red Lion*, 395 U.S. at 400. The fiberoptic BIAS market is also shaped by countless

[45] Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* 40 (2013) ("The law gave cable a subsidy—in the form of a preferential rate on access to telephone poles—that is still in place today.").

[46] *See, e.g.*, *1946: First Mobile Telephone Call*, AT&T http://www.corp.att.com/attlabs/reputation/timeline/46mobile.html (last visited Sept. 18, 2015) (discussing Bell Lab engineer D.H. Ring's invention of the cell phone utilizing radio transmitters and technology).

state and federal subsidies.[47] Today's BIAS market is inseparable from the government policies that enabled, and continue to enable, its existence.

As a result of such reliance on existing cable and radio infrastructure, the market for broadband service has developed as invariably local, guarded by significant barriers to entry,[48] and resembles a monopoly or, at least, oligopoly.[49] New competitors can offer Internet services only by building new networks from scratch. Incumbent communications companies have used this first-to-market, government-enabled advantage to establish a captive customer base for Internet services.[50] Additionally, switching costs are high and consumers are unlikely to be able to determine whether lag, jitter or other service issues are due to providers unduly interfering with their data. *See Verizon*, 740 F.3d at 646-47.

---

[47] Bruce A. Kushnick, *The Book of Broken Promises: $400 Billion Broadband Scandal & Free the Net* (2005).

[48] *Ex Parte* Submission of the U.S. Dep't of Justice at 7, *Economic Issues in Broadband Competition, A National Broadband Plan for our Future* (GN Docket No. 09-51) (Jan. 4, 2010), *available at* http://www.justice.gov/atr/public/comments/253393.htm.

[49] *See id.* ("[T]he Department does not expect to see a large number of suppliers."); *id.* at 11 ("[L]arge economies of scale . . . preclude having many small suppliers and thus often lead to oligopolistic market structures.").

[50] *See* Prepared Remarks of FCC Chairman Tom Wheeler, *The Facts and Future of Broadband Competition 4* (Sept. 4, 2014), *available at* https://www.fcc.gov/document/chairman-remarks-facts-and-future-broadband-competition ("Once consumers choose a broadband provider, they face high switching costs that include early-termination fees, and equipment rental fees. And, if those disincentives to competition weren't enough, the media is full of stories of consumers' struggles to get ISPs to allow them to drop service. ").

The result is that only 37% of Americans have a choice between two or more broadband providers (those providing a download speed of 25 Mbps or better[51]), and only 9% can choose among three or more.[52] The majority of Americans must contract with the sole provider in their area, or settle for a subpar connection.

Accordingly, as recognized by this court in *Verizon*, broadband providers have the ability and incentive to collect fees from content providers to either disadvantage a competitor or provide prioritized access to the network's customers. *Verizon*, 740 F.3d at 645-46 (finding Commission's "speculation" about paid prioritization and other anticompetitive incentives "based firmly in common sense and economic reality"). And because consumers have little choice among ISPs—should they even be able to discern such content discrimination—this ability to interfere with third-party services, applications, and content remains artificially, and dysfunctionally, insulated from market forces.

---

[51] Fed. Commc'ns Comm'n, *FCC Chairman Tom Wheeler: More Competition Needed in High-Speed Broadband Marketplace* (Dec. 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-329160A1.pdf.

[52] David N. Beede, U.S. Dep't of Commerce, *Competition Among U.S. Broadband Service Providers* (Dec. 2014), *available at* http://www.esa.doc.gov/sites/default/files/competition-among-us-broadband-service-providers.pdf.

II. First Amendment Principles Weigh in Favor of the Open Internet Order.

Petitioner Alamo and some *amici* suggest that the Order violates the First Amendment. They are incorrect.

The Order implicates the competing First Amendment interests of individual users to speak and seek speech online, and of ISPs to transmit speech without undue government interference. When the regulation of a communications medium reflects a tension between these interests, the Supreme Court has provided a roadmap for resolving that tension. The FCC has followed that map here. Because the Order furthers a paramount public interest by preserving freedom of speech in a dysfunctional, government-enabled industry, and does so without significantly burdening the speech of ISPs, it should be upheld.

A. The Order Constitutionally Regulates ISPs in Their Role as Conduits for Internet Speech.

Because ISPs (1) operate as conduits for others' speech, and (2) do so via government-provided monopolies and infrastructure, Supreme Court precedent supports the Order's constitutionality. The Order's regulation of broadband Internet access is governed by *Turner Broadcasting System, Inc. v. FCC*, and *Red Lion*. Both *Turner* and *Red Lion* stand for the proposition that tailored, fact-bound regulation of government-enabled mass media designed to promote a diversity of

speech and speakers can not only survive intermediate scrutiny, but vindicate First Amendment rights.

First, and most importantly, the Order regulates ISPs only when they act as *conduits*, rather than creators or endorsers, of information. The Order thus places only nominal restrictions on the expressive activities of ISPs.

Many ISPs play two roles: providing access to the Internet writ large and hosting their own content. For example, Verizon both provides Internet services and hosts its own speech on its website. The Order regulates Verizon and other ISPs in the former role as conduits of information,[53] and not in the latter. *See Associated Press v. United States*, 326 U.S. 1, 20 n.18 (1945) (distinguishing between the AP's editorial and distributive roles). There is no evidence that ISPs endorse speech—besides their own—that passes over their networks. In fact, Petitioners insist that they do *not* exercise editorial discretion in this way.[54]

Thus, the Order on its face does not substantially burden ISPs' First Amendment rights because acting as a conduit *in itself* is not expressive. In *Turner*, the Court recognized that the cable television companies exercised their editorial capacities only to select programming, and otherwise served as "conduit[s] for the

[53] *See* Order ¶ 270 (explaining that ISPs are only being regulated in their roles as conduits).

[54] *See* Joint Brief for Verizon & MetroPCS at 43, *Verizon v. FCC*, (No:11-1355) (July 2, 2012), 2012 WL 9937411, at *43 (stating that ISPs "allow all content in an undifferentiated manner"),

speech of others, transmitting it on a continuous and unedited basis to subscribers." 512 U.S. at 629. Even in the cable TV context, where companies actively select programming, the Court found "little risk that cable viewers would assume that the broadcast stations carried on a cable system convey ideas or messages endorsed by the cable operator" and that therefore, the must-carry rules did not burden expression. *Id.* at 655. The Order applies only to services that allow customers to reach "substantially all Internet endpoints." *Id.* In doing so, the Order limits itself to regulating those ISPs that already hold themselves out as neutral conduits to all speech. Thus, the expressive interests here are no more present than they were in *Turner*.

This last point is worthy of emphasis—amici are civil liberties organizations largely devoted to, and responsible for, the robust application of the First Amendment to online speech. This includes unconditional support for the Supreme Court's holding that speech should not receive compromised protection simply because it occurs online. *See, e.g., Reno*, 521 U.S. at 870 (finding "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium").

The Court in *Reno* properly discerned that the nature of the Internet does not justify content-based restrictions on expression. But that holding does not apply to the Order, which does not regulate content providers but rather *access* to the

content they provide. Indeed, *Reno*'s preservation of an online marketplace "as diverse as human thought" would be substantially diminished if Americans could not access this wealth of speech. It is this gatekeeper role, not the speech beyond that gate, that provides a basis for regulation:

> Although a daily newspaper and a cable operator both may enjoy monopoly status in a given locale, the cable operator exercises far greater control over access to the relevant medium. A daily newspaper, no matter how secure its local monopoly, does not possess the power to obstruct readers' access to other competing publications . . . .

Turner, 512 U.S. at 656. ISPs, as gatekeepers to the online world, function much more like cable companies than newspapers. Regulation of ISPs as neutral common carriers is therefore proper, and indeed necessary to ensure individuals retain a meaningful right to create, access, and view the online content protected in *Reno*.

ISPs are a proper target of common carrier regulation because their industry is built atop existing common carrier infrastructure dependent on exclusive rights provided by the government. *Compare CBS, Inc v. FCC*, 453 U.S. 367 (1981), *and Metro Broad., Inc. v. FCC*, 497 U.S. 547 (1990), *overruled on other grounds by Adarand Constructors, Inc. v. Pena*, 515 U.S. 200 (1995) (permitting regulation of communications entities enjoying monopoly power due to government assistance), *with Miami Herald Pul'g. Co. v. Tornillo*, 418 U.S. 241 (1974), *Buckley v. Valeo*, 424 U.S. 1 (1976), *and First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765 (1978)

(refusing to allow regulation of industries that did not have government assistance in gaining market power). ISP control of the Internet is "compounded by the increasing concentration of economic power in the cable industry." *Turner*, 512 U.S. at 632-33. As discussed above, BIAS is dominated by a handful of incumbents that achieved their power thanks to government policy. The resulting "undue market power," as well as unfair competition exacerbated by horizontal and vertical integration,[55] were also hallmarks of the cable industry when *Turner* was decided. *Turner*, 512 U.S. at 633.

In addition, wireless broadband access operates over frequencies on the electromagnetic spectrum—and is dependent on government auctions of this scarce resource.[56] In *Red Lion*, the Court upheld rules mandating that radio stations give air time to opposing viewpoints against their commercial interests, in part, because "broadcast frequencies constitute[] a scarce resource whose use [can] be regulated and rationalized only by the Government." 395 U.S. at 376. Just as the scarcity rationale permitted the regulation of broadcast radio "in a manner responsive to the

[55] *See* 2010 Open Internet Order ¶ 21 n.46 (noting vertical integration of ISPs).

[56] The FCC's recent auction for mid-band spectrum generated $44.9 billion, showing increasing demand for this public resource. Marguerite Reardon, *FCC Rakes in $45 Billion from Wireless Spectrum Auction*, CNET (Jan. 29, 2015), http://www.cnet.com/news/fcc-rakes-in-45-billion-from-wireless-spectrum-auction/.

public convenience, interest, or necessity," so too does it permit the Open Internet Order. *Id.* at 377 (quotation marks omitted).

Because BIAS operates through the cable lines and wireless spectrum, the FCC's Order is not only permissible, it is necessary "to impose order upon a market in dysfunction" and protect free speech. *Turner*, 512 U.S. at 635.

B. The Open Internet Order Is Facially Content-Neutral and Survives Intermediate Scrutiny.

The Order's three bright lines forbid ISPs from blocking access to legal content,[57] throttling data on the basis of content, or prioritizing certain traffic in exchange for payment or to benefit an affiliated entity.[58] These rules properly ensure that Internet providers do not curb "the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences." *Red Lion*, 395 U.S. at 390. However, in regulating a medium of communication imbued with First Amendment interests of its own, the Order merits meaningful scrutiny.

The standard for that scrutiny can be found in *Turner*. There, the Court

[57] The core of the Order prevents discrimination based on the content of speech carried over the network. In guidance, however, the Order also reasserts the FCC 's "tentative conclusion" that ISPs may make "reasonable efforts to address the transfer of unlawful content or unlawful transfers of content" where they see fit. Order ¶ 304. It would raise serious constitutional concerns to construe the Order to delegate to ISPs the decision as to which content is lawful.

[58] *See* Order ¶¶ 7-8.

upheld the FCC's "must-carry" rules, which required cable television companies to devote a portion of their channels to local broadcast stations. 512 U.S. at 626. The Court recognized that the cable companies engaged in limited programming selection, and otherwise served as "conduit[s] for the speech of others, transmitting it on a continuous and unedited basis to subscribers." *Id.* at 629. Ultimately, the Court ruled that the must-carry rules were created "without reference to the content of speech." *Id.* at 643. Having made this determination, the *Turner* Court found that intermediate scrutiny was proper: the Order must (1) further a substantial government interest, and (2) not burden substantially more speech than necessary to accomplish it. *Id.* at 662.

Like *Turner*'s must-carry rules, the Order is unrelated to the content of speech, and is thus content-neutral. The Order thus merits, and meets, the same scrutiny.

The government interests furthered by the Order are nothing short of compelling: (i) preserving the public benefits of the 21st century's preeminent communications system; (ii) "promoting the widespread dissemination of information;" and (iii) facilitating fair competition in the communications market. *See Turner*, 512 U.S. at 663 ("[W]e have no difficulty concluding that each of [these] is an important government interest."). The substantiality of the interests furthered by the Order is, quite simply, self-evident. The question is whether the

Order furthers these interests without unduly infringing upon the right of ISPs to engage in expression protected by the First Amendment. It does.

Most critically, the editorial interests impacted by the Order are even *less* present than those in *Turner*. Because it regulates only ISPs that offer access to "substantially all Internet endpoints," their interest in editorial culling is far less present than in *Turner*. Unlike in *Turner,* where the Court blessed local TV station's intrusion into curated cable packages, the associated limits on ISPs' editorial interests are difficult to discern. Because the First Amendment concerns of ISPs are "at best speculative," the Order suppresses no more speech than is permitted. *See Red Lion*, 395 U.S at 393.

Moreover, considering the enormity of the interests at stake, *see supra* II.B, and the sizeable power of ISPs to regulate users' speech—and therefore, society's marketplace of ideas—there is no less invasive or more effective method than to mandate that ISPs act as common carriers. The First Amendment interests of individual users cannot be vindicated with a partial solution in a non-competitive market that permits even some forms of discriminatory content delivery—those likely invisible to the user.

III. The Primary Guideposts for Any "Unreasonable Interference" Analysis Should Be Free Expression and Application Agnosticism.

The meaningful exercise of our constitutional rights—including the freedoms of speech, assembly, and press—has become dependent on broadband

Internet access. Accordingly, the touchstone of the Order must be whether it preserves and promotes opportunities for online expression. As explained above, the Order, and its bright-line rules, do so.

The Order's additional guidance regarding the "rule of general conduct" or "unreasonable interference" rule, however, raises First Amendment concerns because of its sheer complexity.[59] This guidance includes seven factors to weigh in assessing whether particular practices run afoul of the bright-line rules: impact on competition; impact on innovation; impact on free expression; impact on broadband deployment and investments; whether the actions in question are application-specific; whether they comply with industry best standards and practices; and whether they take place without the awareness of the Internet subscriber. While each is potentially objective, the Commission nevertheless has significant discretion to weigh these factors in every case. Accordingly, the burden on regulated providers in litigating such cases *ad hoc* could discourage innovation and impede the Internet's continued growth as a platform for speech, commerce, and social activity.

Federal courts should, where possible, construe ambiguous regulations so as to avoid constitutional concerns. *See, e.g. Clark v. Martinez*, 543 U.S. 371, 381 (2005); *Ashwander v. Tenn. Valley Auth.*, 297 U.S. 288, 347 (1936) (Brandeis, J.,

[59] Order ¶ 21.

concurring). Here, to avoid First Amendment concerns, *amici* urge the Court to authoritatively construe the "general conduct" rule as a simpler assessment of whether the practice at issue promotes or hinders free expression, and whether the practice is "application agnostic." Doing so will ensure that the general conduct rule is tailored to its core purposes—without creating a vague standard.

The free expression impact factor is the rationale for the Order itself, and its primacy needs no justification. Application agnosticism, meanwhile, is an objective standard that the Commission, providers, and courts can readily apply. The Order defines an application-agnostic ("AA") practice as one that "either does not differentiate in treatment of traffic or, if it does so, differentiates without reference to content, application or device."[60] As Professor Barbara van Schewick has explained, an application-agnostic standard would forbid providers from treating

> YouTube differently from Hulu, or the website of the New York Times differently from the website of the Wall Street Journal or Free Press. Nor would [they] be allowed to treat online video differently from e-mail, treat applications that use the BitTorrent protocol differently. . . . But [they] would be allowed to treat data packets differently based on criteria that have nothing to do with the application or class of application.[61]

---

[60] Order ¶ 144 n.344.

[61] Barbara van Schewick, *Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like,* 67 Stan. L. Rev. 1 (2015).

Service providers can still manage congestion, offer varying tiers of service and products—they simply cannot target specific applications for different handling.

AA vindicates the interests of both speech and innovation. By definition, application-agnostic practices are unlikely to disfavor certain sites, applications, or services based on content; in other words, AA is content-neutral. They are also less likely to create unfair barriers to innovation, because they help ensure that users can access new sites, services and applications on the same terms as established ones. The marketplace of ideas should decide which applications and speech rise to the top.

AA also largely incorporates the other guiding factors. An application-agnostic practice is highly likely to promote competition and protect consumers, because it ensures that users, rather than providers, decide what content to favor. Indeed, AA may be the most effective way to promote end-user control. For example, the Order suggests that "transparent" practices might pass muster under this factor, but in practice transparency is a poor substitute for meaningful choice. Providers may simply ask users to agree to complex contracts in which they unknowingly sign away many of their rights and interests, and then claim that the users consented to the providers' practices. As long as such contracts of adhesion are upheld as fair bargains by the courts, "user control" is unlikely to hold much weight as an independent factor.

Amici understand the Commission's desire to address unforeseen practices that may undermine the Open Internet. Tying the rule closely to free expression and application agnosticism will provide much-needed certainty and further the Order's three bright-line rules.

CONCLUSION

"The First Amendment's command that government not impede the freedom of speech does not disable the government from taking steps to ensure that private interests not restrict, through physical control of a critical pathway of communication, the free flow of information and ideas." *Turner*, 512 U.S at 657. The Order narrowly and effectively ensures the continued free flows of ideas through the Internet, and should be upheld. However, amici urge the Court to provide guidance to the FCC regarding the rule of general conduct, to offer greater certainty to providers and users alike.

Dated: September 21, 2015

Respectfully submitted,

/s/ Corynne McSherry

Corynne McSherry
Kit Walsh
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
Telephone: (415) 436-9333
corynne@eff.org

Counsel for Electronic Frontier Foundation

Lee Rowland
Samia Hossain
AMERICAN CIVIL LIBERTIES UNION
125 Broad Street
New York, New York 10004
Telephone: (212) 549-2550
lrowland@aclu.org

Counsel for American Civil Liberties Union

Arthur B. Spitzer
AMERICAN CIVIL LIBERTIES UNION
OF THE NATION'S CAPITAL
4301 Connecticut Avenue
Washington, D.C. 20008
Telephone: (202) 457-0800
artspitzer@aclu-nca.org

Counsel for American Civil Liberties Union of the Nation's Capital

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of *Amici Curiae* Electronic Frontier Foundation, American Civil Liberties Union, and the American Civil Liberties Union of the Nation's Capital in Support of Respondents complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,923 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: September 21, 2015

By: /s/ Corynne McSherry

Corynne McSherry
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Tel: (415) 436-9333
corynne@eff.org

Counsel for Amicus Curiae

CERTIFICATE OF FILING AND 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 D.C. Circuit by using the appellate CM/ECF system on September 21, 2015. Service of the foregoing will be made electronically via the appellate CM/ECF system upon the participants in the case who are registered CM/ECF users. Service on the counsel listed below will be made by U.S. Mail.

Mr. Robert S. Schwartz
Constantine Cannon LLP
1301 K Street, NW
Suite 1050 East
Washington, DC 20005

Mr. Rick Charles Chessen
National Cable & Telecommunications Association
25 Massachusetts Avenue, NW
Suite 100
Washington, DC 20001-1431

Mr. Sam Kazman
Competitive Enterprise Institute
1899 L Street, NW
12th Floor
Washington, DC 20036

Mr. Kellam McChesney Conover
Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, NW
Washington, DC 20036-5306

Dated: September 21, 2015

/s/ Corynne McSherry
Corynne McSherry

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amicus Curiae

Appendix A

JOINT STATEMENT OF INTERNET ENGINEERS AND PIONEERS

The undersigned submit the following statement in support of the Open Internet Order. We seek to assist the Court's review of the Order by supplying certain facts about the structure, history, and evolving nature of the Internet. As developers, engineers, and designers, we realize that without openness and neutrality the Internet as we know it will cease to exist, because it is that openness and neutrality that gives the Internet its flexibility, leads to its growth, and has made it a vital resource for all aspects of modern life. We believe the Order, if affirmed by this Court, will help preserve those characteristics. Further, in the absence of a clear but limited Open Internet Rule, service providers could *and would* continue to engage in the practices of blocking, throttling, and interference. These practices would upend the Internet, making development of new protocols and services dramatically more difficult, breaking existing protocols and services, and even introducing security vulnerabilities that would not have been present without service provider interference. In short, without a clear but limited Open Internet Rule, the rapid pace of innovation the Internet has experienced over the last forty years could come to a disastrous halt. We urge the Court to uphold the Order.

I. A Brief Introduction to the Internet

A. A Network of Networks

Fundamentally, the Internet is a collection of tens of thousands of individual networks of computers and other devices, almost all of which are owned, operated, and maintained by different entities.[1] In order to facilitate global communication, each of these independent networks interconnects to one or more of the other

[1] CIDR REPORT, www.cidr-report.org/as2.0/ (last visited Sept. 14, 2015).

networks, thus leading to the term "Internet." While each of these networks speaks the same language (or in technical parlance, protocol), and can thus be described using the same technical tools, the actual forms of the networks vary widely, both in terms of their architecture (i.e. their size and shape) as well as the underlying technology they use to connect devices. These differences depend in large part on the purpose each network serves.

For example, the type of network that is perhaps most familiar is a Local Area Network (LAN). LAN networks, such as the wired network in an office building or a Wi-Fi network in a home, connect a relatively small number of devices together. LAN networks connect to the Internet via yet another network, that of an Internet service provider, or ISP.

A typical ISP network connects anywhere from dozens to thousands of homes and businesses (or in the case of some wireless ISPs, mobile devices) to the rest of the Internet. This connection occurs in two parts. In the first part, the ISP must connect its customers (i.e. its retail subscribers) within a given geographic area to its own network facilities. This connection can be made over a variety of mediums: coaxial cables (originally used solely for cable TV transmission), copper wires (originally used solely for telephone communication), fiber optic cables, or in the case of wireless ISPs, radio waves. For most communications mediums ISPs configure the connection to be asymmetric: ISPs reserve more of the capacity of the connection (i.e. bandwidth) for downloads – data traveling to the customer – than it does for uploads from the customer.[2]

---

[2] Note that many ISPs do not configure fiber connections to be assymetric, with the exception of some residential GPON.

The second part of the connection involves connecting the ISP's network to one or more of the other networks that make up the Internet. Typically, this second connection is made to either another ISP or an entity known as a "backbone provider." Unlike a retail ISP, a backbone provider does not sell Internet access to individuals. Instead, backbone providers are "high capacity long-haul transmission facilities" which offer to connect different networks together in what are called "peering arrangements."[3]

In peering arrangements, the two connecting parties formalize the role each will play in their interconnection: what levels of traffic will be allowed to and from each party, where the interconnection will be located physically, and who will pay for upgrades to the interconnection if they are necessary. Peering between large entities is often done in a settlement-free manner, meaning that no money is exchanged as part of the peering arrangement. This sort of settlement-free peering is sometimes dependent on the two networks exchanging similar levels of traffic (i.e. each network sending as much traffic to the other as it receives).[4] However, an equal traffic exchange requirement frequently does not make much sense when backbone providers or edge providers connect to ISP networks, due to the inherent asymmetric nature of ISP traffic. In other words, because most ISP customers download more than they upload, any peering arrangement between a backbone or edge provider and a retail ISP's network will result in more traffic being sent from the backbone or edge provider to the ISP than vice versa.

---

[3] *Verizon Communications and MCI, Inc. Applications for Approval of Transfer of Control*, 20 FCC Rcd 18433, 18493 (2005).

[4] *See, e.g., Time Warner Cable's IPV4 and IPV6 Settlement-Free Peering Policy*, TIME WARNER CABLE, http://help.twcable.com/twc_settlement_free_peering_policy.html (last visited Sept. 14, 2015).

Finally, it should be noted that the same company will often act in different roles: a large ISP can provide backbone service to other, smaller ISPs, and also provide edge connections to individual customers. Also, a large edge provider may own similar infrastructure to a backbone provider. Thus, it is important when discussing the roles of the major players on the Internet to focus on the specific context in which they are being discussed; to do otherwise can lead to confusion and mismatched assumptions.[5]

B. Packet-Switching and Congestion

While the above gives an accurate picture of how the Internet is laid out, it does not explain how the different networks actually succeed in communicating with one another. In this section we explain how this is done, so that we can later explain the technical ramifications of the FCC's Order.

Two major technical principles underlie how the Internet functions. The first is the concept of packet switching. In a packet switched network, the data to be transmitted (be it a webpage, images, sound files, or a video) is broken down into chunks known as packets, each of which is sent off individually to its destination.[6] An Internet packet contains several important pieces of information: the numerical address of the device which sent the packet, known as an Internet Protocol address (or IP address); the IP address of the intended recipient; the type of data the packet

---

[5] For example, an ISP may have different customers depending on its role: as a retail ISP, its customers are the retail customers who subscribe to its service for Internet access, but if it also provides transit services as a backbone provider, then in that role its customers would be other ISPs.

[6] JONATHAN E. NEUCHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 42-43 (2005).

contains; and of course the actual data.[7] In this way, a packet is similar to a postcard—anyone who is part of the delivery chain can read who it is intended for, who sent it, and what it says. (Note that this does not hold true if the contents of the packet are encrypted—then the packet is more like a postcard where the message is written in code only the sender and receiver can understand.)

When it comes time for a computer to transmit a packet, the computer sends it to the next "hop" in the delivery chain, typically a network device known as a "router." A router is a specialized device that bridges the connection between multiple communications links, whose sole job is to send packets one step closer to their destination. It does this via a "routing table," which lists all the communication links the device is attached to, and the range of IP addresses that can be found on each of those links. Thus when a packet arrives, the router compares its destination address to the routing table and then sends it off on the appropriate link.

Of course, sometimes packets arrive at a router faster than the router can process them or faster than the communications link can transmit them, leading to congestion. Internet congestion is analogous to the traffic congestion that might occur when a busy four-lane interstate splits into two smaller highways: even though there is theoretically enough capacity, if all of the cars coming from the interstate want to travel along only one of the smaller highways, a backup will ensue. Similarly, if a router receives packets faster than it can transmit them along their desired links, the packets will be stored in a buffer until they can be sent. Unlike traffic congestion, however, if too many packets fill up the buffer, any new

---

[7] INFO. SCI. INST., UNIV. S. CAL., DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION (1981), *available at* https://tools.ietf.org/html/rfc791.

packets will simply be "dropped", or discarded. Thus the Internet is a "best-effort" service: devices make their best effort to deliver packets, but do not guarantee that they will succeed.[8]

C. The Principles of Neutrality and Openness Are Key Features of the Internet's Design

The Internet is more than just a way for computers across the globe to exchange packets of data; it is a platform on which people have developed a variety of amazing new technologies, from web browsing to email to social networking to online courses. The Internet's tremendous growth and popularity as a platform have been due at least in part to two design principles, both of which ensure that the Internet is an open, neutral platform.

The first of these design principles is the idea of the layered network communications stack (often referred to as simply "the network stack"). Essentially, the network stack is a way of abstracting the design of software needed for Internet communication into multiple layers, where each layer is responsible for certain functions, but can implement those functions in any way that meets the specifications. For example, the "physical layer" is responsible for physically transmitting and receiving bits. It can do so over fiber optic cable, copper telephone lines, radio signals, etc., as long as it provides a way for the layer above it to access the "transmit and receive bits" function. Further up the stack is the "internetwork layer," which is responsible for ensuring each device on the network

---

[8] In fact dropping packets is one of the key signals routers use to communicate to devices that they are sending packets too quickly, so that the devices can reduce their transmission rate. Thus, communication software uses dropped packets as an indication that they are sending too rapidly, and should reduce their transmission rate to keep the Internet from collapsing from excessive congestion.

has a unique address, and for sending and receiving packets of data to specific addresses. It is at this layer that the famous Internet Protocol actually resides, which provides a "send data to a certain address" function to the layer above. Similarly, further up is the "transport layer," which is the layer that is usually exposed to applications in order to send data to other devices. This is the layer at which the also well-known Transmission Control Protocol (TCP) resides, which is responsible for ensuring that data gets to its destination reliably and intact.[9]

The key takeaway from the idea of the network stack is that the specification is well-defined enough for a developer to understand how her protocol will interact with the rest of the network stack, while at the same time flexible enough to allow for different implementations and widely-varying uses cases (since each layer can tell the layer below it to carry any type of data). This is why the same Internet Protocol can support such varied applications as email and real-time video-conferencing. If someone wants to develop a new Internet application or protocol, all they have to do is insert their new technology at the appropriate layer; the layers below will perform their functions regardless of the type of data the developer tasks them to handle. This openness allows developers to build new and different types of applications without having to worry about the technical details of the layers below. "Consider, for instance, how these design principles collectively facilitated the rise of the World Wide Web application. Because the network is general, its founder Tim Berners-Lee could introduce it without requiring any

---

[9] DOUGLAS E. COMER, INTERNETWORKING WITH TCP/IP VOLUME ONE (6th ed. 2013). Note that for simplicity of explanation, some of the layers have been omitted, such as the link layer (which sits between the physical layer and the network layer).

changes to—or permission from—the underlying physical network."[10] All he had to do was define the protocol, and the underlying layers transported the data as desired.

The second design principle is the "end-to-end principle." In order for a network to be general purpose, the nodes that make up the interior of the network should not assume that end points will have a specific goal when using the network or that they will use specific protocols; instead, application-specific features should only reside in the devices that connect to the network at its edge.[11]

It is easy to see how the end-to-end principle applies in the case of the Internet. The interior of the network, made up of the communications links (i.e. the physical cables) and the routers that connect them, originally did very little processing or modification of the packets they handled.[12] In fact, the Internet Protocol, which is the protocol routers use to communicate, does not even have a way for a device to make sure a packet arrived at its final destination. All the Internet Protocol requires is for a router to read incoming packets, figure out the

---

[10] Brief Amicus Curiae of Internet Engineers and Technologists Urging That The FCC's Order Be Affirmed, Verizon v. Federal Commc'ns Comm'n, 740 F.3d 623 (D.C. Cir. 2014) (No. 11-1355).

[11] J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277 (1984).

[12] We note that many network operators and equipment vendors contest the fundamental nature of the "end-to-end" principle. However, their arguments are usually made in order to claim that they (or their equipment) can "add value" to the network by adding "smarts" to the network itself—usually as a way to try to reverse the commoditization of network hardware and services. Further, as we explain in section III.C, this insertion of "smarts" into the interior of the network frequently causes problems for developers of innovative new protocols and applications designed to run on a neutral Internet.

next hop along their path, and send them off. The actual specialization comes entirely from the computers and servers and smartphones that connect at the "edge" of the Internet. This is how the Internet can support protocols that require guaranteed delivery of data (such as file transfer protocols), as well as protocols where guaranteeing delivery is less important than ensuring that the packets that are received have low latency (such as protocols for voice or video chat).

II. How the Internet Has Changed Since 2010

While technologies like the Internet Protocol and TCP have changed little since the early nineties, part of the Internet's resilience and value comes from the myriad ways in which those underlying protocols can be used. It should come as no surprise, then, that the Internet as a whole is not a static, monolithic creation, but a constantly evolving system. In this section, we describe the major ways the Internet as a whole, and consumer ISPs in particular, have changed since 2010.

A. New Internet Protocols and Services Continue to be Invented

Although it may seem obvious, it is worth noting that new services and applications that rely on the Internet are constantly being developed. For example, take the continuing rise of the "Internet of Things," a term used to describe the increasingly Internet-connected nature of objects in our environment that were not traditionally thought of as Internet-connected computers.[13] Typical examples include everything from Internet-connected home appliances to wearable devices (including fitness and health-tracking devices), and even Internet-connected

---

[13] Bonnie Cha, *A Beginner's Guide to Understanding the Internet of Things,* RE/CODE, Jan. 15, 2015, http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/.

automobiles. Many of these devices use the Internet in novel ways, and could be seriously affected by blocking or throttling based on protocol or service.

Additionally, innovation surrounding the Internet is not limited to new services which use existing protocols to communicate via the Internet. Current innovation goes even deeper, down the network stack to new protocols and fundamentally new ways of using the network. For example, the "InterPlanetary File System (IPFS) is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files,"[14] first developed just last year.[15] The goal of IPFS is to create a more permanent, more distributed version of the World Wide Web, one in which the entirety of files available on the Web are distributed to millions of computers across the globe. If successful, IPFS would make censorship of individual webpages or websites technically impossible, while also ensuring that a permanent record of all the files ever posted on the Web is always available, for archival and historical purposes. IPFS relies on the underlying decentralized, open infrastructure of the Internet, distributing data using peer-to-peer protocols that are fundamentally different from the sorts of protocols used to transmit webpages, emails, or streaming videos.

The key takeaway from these examples is that innovation surrounding the Internet is ongoing—but more importantly, this sort of innovation relies on the open, neutral nature of the Internet. As we explain further in section III.C, if ISPs interfered with their customers' traffic based on the protocol or service in use, such innovation would become impossible.

---

[14] THE IPFS PROJECT, https://ipfs.io/ (last visited Sept. 14, 2015).

[15] *History for IPFS*, GITHUB, https://github.com/ipfs/ipfs/commits/master/README.md (last visited Sept. 14, 2015).

B. ISP Caching is Becoming Less Useful

In the early days of the Internet, many ISPs set up caching servers that would sit between their customers and the rest of the Internet. These servers would record what data customers were requesting from the World Wide Web, and store copies in a local cache that the server could send when other customers made the same request. For example, if many customers were reading the same newspaper article about net neutrality, the ISP would store a copy of that article on the caching server. Then, when a new request for the article came in, the ISP would send back the copy instead of waiting for the request to go all the way to the newspaper's server and back via the Internet. This way the ISP could reduce the amount of time it took for a customer to download the article (since the ISP's caching server would be closer to the customer than the newspaper's server), and ISPs could save on bandwidth (since they would not have to re-download the article from the newspaper's server every time a new request came in).[16]

However, recent changes have decreased the need for ISP caching services. This is due to the widespread use of Content Delivery Networks, or CDNs. CDNs are very similar to the caching servers described above, except they can be (and often are) operated by companies other than ISPs (such as third-party companies who sell their CDN service to edge providers). CDNs consist of Internet-connected caching servers strategically placed in different geographic regions, on the edge of or inside the network of one or more ISPs. Content originators upload their content to these caching servers, so that they can have fine-grained control of what gets

---

[16] JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH (4th ed. 2007).

cached and how long it stays cached—control they do not have over ISP-controlled caches.

In addition to becoming unnecessary, ISP caching is also becoming less feasible due to the increasing proportion of Internet traffic that is encrypted. (In 2010 less than 2% of traffic on the Internet was encrypted[17], but by 2016 that number is projected to reach over 64%.[18]) Encryption prevents ISP caching from being effective because when a user requests a webpage or file over an encrypted connection, the ISP cannot see the name or location of the file the user is requesting, or the contents of the file itself. As a result, the ISP has no way of knowing what files are popular enough to cache, nor any way of knowing when a user requests a popular file. Given the inevitability of ubiquitous encryption, ISP caching is destined to become an obsolete practice.[19]

---

[17] SANDVINE, GLOBAL INTERNET PHENOMENA REPORT (2011), *available at* https://www.sandvine.com/downloads/general/global-internet-phenomena/2011/1h-2011-global-internet-phenomena-report.pdf

[18] SANDVINE, GLOBAL INTERNET PHENOMENA SPOTLIGHT: ENCRYPTED INTERNET TRAFFIC (2015), *available at* https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf.

[19] Indeed, all major browsers have announced that they will only support the next version of the famous HTTP protocol, HTTP/2, over encrypted connections. Dan Goodin, ARS TECHNICA, *New Firefox Version Says "Might as Well" to Encrypting All Web Traffic,* April 1, 2015, http://arstechnica.com/security/2015/04/new-firefox-version-says-might-as-well-to-encrypting-all-web-traffic/

C. DNS and Email Are No Longer the Province Solely of ISPs

Another major change has been the dramatic surge in popularity of third-party web-based email providers. For example, consider US email providers. Over the last month, Google, Microsoft and Yahoo (the top three in the US) were ranked third, fifth, and seventh in the world in terms of volume of email sent. For comparison, the top three US ISPs, Comcast, AT&T, and Time-Warner Cable ranked 13th, 55th, and 22nd.[20] While not all of the email coming from those domains is generated by customers, the dramatic difference in popularity illustrates the decreasing relevance ISP customers put on the information services provided by their ISPs.

Similarly, fewer people are making use of their ISP's Domain Name Services (DNS)[21] for reasons of speed or security. [22] This is because of the proliferation of free, open DNS servers online. Google Public DNS, for example, is a DNS service Google offers to any Internet user, free of charge, which handles over 400 billion DNS requests per day.[23]

---

[20] *Email Overview – SenderBase,* CISCO, https://www.senderbase.org/static/email/#tab=2 (last visited Sept. 14, 2015). Note that some companies are listed under multiple organizational names; when cited above, we have provided the highest ranking for a given company.

[21] DNS is the service computers rely on to look up the numerical IP address associated with a given domain name (e.g., www.eff.org).

[22] *Introduction to Google Public DNS,* GOOGLE, https://developers.google.com/speed/public-dns/docs/intro (last visited Sept 14, 2015).

[23] Yunhong Gu, *Google Public DNS and Location-Sensitive DNS Responses,* GOOGLE WEBMASTER CENTRAL BLOG, Dec. 15, 2014, http://googlewebmastercentral.blogspot.com/2014/12/google-public-dns-and-location.html.

D. Customers Now Depend on ISPs for Internet Access, Not Information Services

In the early days of Internet access, customers frequently chose which ISP to subscribe to based on the content and information services that ISP supplied in addition to general Internet access. ISPs like AOL, Compuserve, or Prodigy differentiated themselves based on the different information services each provided—services like chat rooms, bulletin board systems, email, and specialized content only available to an ISP's own subscribers.[24]

Now, however, ISPs compete primarily on the reliability and bandwidth of their Internet connections,[25] and customers subscribe to an ISP's service not because of the added information services an ISP might provide, but because the subscription enables customers to transmit and receive data to and from the wider Internet. In other words, the information services ISPs provide are simply no longer connected in any meaningful way to the data routing and transmission service they offer. The two are easily separated, as evidenced by the fact that a consumer can instead choose to subscribe to any given information service from an entity other than their ISP. In fact, saying that ISPs provide an information service to their customers because they offer caching and webmail in addition to Internet

---

[24] Michael Wolff (1997). Netstudy. Dell Publishing.

[25] *See, e.g.*, *Sprint 4g Commercial,* YOUTUBE, https://www.youtube.com/watch?v=NPdkvg9Kw-M (last visited Sept. 14, 2015) (touting the bandwidth of Sprint's 4G wireless network); *Comcast- Fast Rabbit*, YOUTUBE, https://www.youtube.com/watch?v=h16qMJ_LCyg (last accessed Sept 14, 2015) (compares Comcast's high-speed Internet access with "a rabbit/panther with turbines backed by an unusually strong tailwind on ice…driven by an over-caffeinated fighter pilot with a lead foot all traveling down a ski jump in Switzerland under better than ideal conditions.").

connectivity is like saying that airlines are in the business of providing an entertainment service because they offer in-flight movies in addition to transportation. While these additional services might be selling points, they are not integral to the fundamental offering ISPs and airlines make: to transport things (either data or people) at the customer's request.

III. Technical Interpretation of the FCC's Order

In light of the foregoing, we can better anticipate the technical consequences of the Order and the risks of losing the "rules of the road" it establishes. We focus on the parts of the Order that will have the greatest technical effect: the rule preventing broadband ISPs from slowing down traffic (or blocking it altogether) based on what type of data the traffic contains, the source of the traffic, or the type of Internet service the traffic carries; and the rule preventing broadband ISPs from prioritizing certain types of traffic in exchange for consideration (monetary or otherwise).

A. Technical Effects the Order Will *Not* Have

First, we wish to dispel the rumor that the FCC's Order will eviscerate ISPs' ability to manage their networks, resulting in massive congestion, unchecked proliferation of spam and viruses, and slow speeds for all.[26] This is simply not the case. The Order contains an exception for reasonable network management. Thus, as the FCC has explained, it does not affect ISPs' ability to filter unwanted spam,

---

[26] *See, e.g.*, *The Truth About Net Neutrality*, CENTER FOR INDIVIDUAL FREEDOM, http://www.stopnetregulation.org/wp-content/uploads/2011/08/Net-Neutrality-talking-points.doc.pdf (last accessed Sept. 14, 2015) ("Under 'Net Neutrality' regulations, every decision to block pornography, spam, or security threats will have to be approved by the government.").

computer viruses, and other malicious content out of their customers' unencrypted traffic, if the customer requests this sort of protection.[27] Similarly, it does not bar ISPs from defending their networks against attacks.

Second, the Order does not affect techniques for dealing with network congestion that do not discriminate based on service or application.[28] Such techniques include "weighted fair queuing," in which each flow of traffic (for example, all of the traffic coming to or from each customer) is assigned a proportion of the outgoing bandwidth along the congested portion of the network. More advanced algorithms for handling congestion, such as Comcast's Protocol-Agnostic Congestion Management System are also not impacted by the prohibition on throttling.[29] Simply put, the Order will not dramatically change or hamper how most ISPs manage their networks. ISPs will still be able to ensure each customer gets a fair allocation of the ISP's total bandwidth. And of course, ISPs can still sell customers different levels of service, and manage their network so that higher-paying retail customers get more overall bandwidth. The only thing the Order forbids is ISPs blocking or throttling their customers' traffic based on the content, applications, or protocols their customers choose to use.

---

[27] FED. COMMC'NS COMM'N, REPORT AND ORDER ON REMAND, DECLARATORY RULING, AND ORDER para. 221 (March, 12, 2015), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf.

[28] Monica Alleven, *Nokia Networks: Necessary Network Management Still Possible Under Proposed Net Neutrality Rules*, FIERCEWIRELESSTECH, Feb. 9, 2015, http://www.fiercewireless.com/tech/story/nokia-networks-necessary-network-management-still-possible-under-proposed-n/2015-02-09.

[29] C. Bastian et al., *Comcast's Protocol-Agnostic Congestion Management System*, COMCAST, Dec. 2010, https://tools.ietf.org/html/rfc6057.

B. Scope of the FCC's Order

Some opponents of the Order suggest that it allows the FCC to regulate the entire Internet.[30] This is not the case. The Order is limited in scope, targeting only retail broadband ISPs. With that said, we do not intend to minimize the effects should the Order be struck down; data destined for retail customers make up a huge percentage of U.S. Internet traffic.

Instead, we wish to highlight that unlike large businesses or data centers, which typically have multiple connections to different ISPs in order to achieve redundancy, most retail customers have only one Internet connection. As a result, retail ISPs enjoy what is known as "gatekeeper authority"—they are the sole gatekeepers of what customers can do online, since customers have no way to bypass any blocking or filtering their ISP puts in place (except changing ISPs, which is a time-consuming process that is often not even feasible). Essentially, retail ISPs represent a single control point between a user and all Internet content and services. As with any single point of control, it is possible for an ISP to exert controls that limit what a user can access or do. In the next section, we explain how this weak link could break if the Open Internet rule is struck down.

C. Risks In the Absence of Open Internet Rule

In the absence of a clear and limited Open Internet rule, ISPs will be free to block, throttle, or speed up data based on its content or what service or application generated it. ISPs could degrade (or altogether block) certain protocols, content, or websites. A frequently given example is that of an ISP degrading traffic containing

---

[30] *See, e.g.*, *supra* note 27 at 321 (Commissioner Pai's dissenting statement on the order) ("[The Order] gives the FCC the power to micromanage virtually every aspect of how the Internet works.").

streaming movies from some or all edge providers, in order to encourage its customers to instead use its own media-streaming service. But this sort of blocking and throttling would only be the tip of the iceberg. ISPs could go further, degrading traffic for any service they do not recognize or have not previously approved of.

That, in turn, could violate the principle of openness upon which the Internet was built. Developers would have to ensure that their new application or protocol would work under different specifications on each of the thousands of networks that make up the Internet. Some networks might decide to handle data differently depending on whether it represented webpages or video. Others might decide that certain data needed to be prioritized.[31] Such a haphazard mishmash of different specifications and engineering conditions would have made the growth of the Internet as we know it utterly impossible. Instead, it would have resulted in a balkanized Internet—one in which each ISP was its own private fiefdom, where edge providers had to negotiate with the gatekeeper in order to get access to the end users.

---

[31] It is worth noting that the Internet Protocol does specify a field in the header of IP packets known as the "differential service" field, meant to indicate some sort of priority. However, in the over thirty years since the widespread adoption of IP, no consensus has been reached about how edge devices should populate that field for use on the public Internet (as opposed to within private networks, such as a company's LAN). As a result, traffic prioritization on the *public* Internet is almost nonexistent. The closest the Internet engineering community has come to a standard on prioritization is RFC 2474, which is a *proposed* standard last updated in 1998, and which is not in force. IETF NETWORK WORKING GROUP, DEFINITION OF THE DIFFERENTIATED SERVICES FIELD (DS FIELD) IN THE IPV4 AND IPV6 HEADERS (1998), *available at* https://tools.ietf.org/html/rfc2474.

But blocking and throttling are not the only dangers. ISPs could decide to violate the end-to-end principle, inserting nodes in their network that tried to "enhance" their customers' experience by augmenting or transforming some content. This might seem like a reasonable design, since conceivably an ISP might have access to information that edge providers would not. (For example, an ISP might be able to provide more relevant search results or other information since it has a complete record of its customers' browsing histories.) But this sort of interference could not only introduce bugs into services and webpages that weren't expecting it, it could make it impossible for some applications (including applications yet to be dreamed of) to work correctly. Worse yet, it could also introduce security vulnerabilities which a malicious actor could use to harm the ISP's customers.

IV. Conclusion

As computer scientists, networking engineers, and professionals who deal with Internet technology on a daily basis, we realize that without openness and neutrality the Internet as we know it will cease to exist, because it is that openness and neutrality that give the Internet its flexibility, lead to its growth, and have made it a vital resource for all aspects of modern life.

We also realize that the threat to the Internet's openness and neutrality is real. None of the scenarios described in the previous section is hypothetical. Comcast has interfered with legitimate traffic based solely on its type.[32] Both Comcast and Verizon have also admitted to modifying their customers' traffic

---

[32] Peter Eckersley et al., *Packet Forgery By ISPs: A Report on the Comcast Affair,* ELECTRONIC FRONTIER FOUNDATION, Nov. 28, 2007, https://www.eff.org/wp/packet-forgery-isps-report-comcast-affair.

without their consent—Comcast by inserting ads into the webpages its customers view,[33] and Verizon by inserting unique tracking ID numbers into the data its customers send.[34] Port blocking and interference by ISPs in general has forced developers of new protocols and services to "camouflage" their new protocols as existing ones, in order to avoid discriminatory treatment. In fact, this sort of interference has become so bad that network engineers have developed a name for it: the "ossification" of the network stack.[35] As a result of this interference, development of innovative new protocols and services is already being hindered.[36]

If this sort of blocking, throttling, and interference becomes more widespread, it would transform the Internet from a permission-less environment (in which anyone can develop a new app or protocol and deploy it confident that the Internet treats all traffic equally) into one in which developers would first need to seek approval from or pay fees to ISPs before deploying their latest groundbreaking technology. Developers and engineers would no longer able to depend on the core assumption that the Internet would treat all data equally. The

---

[33] David Kravets, *Comcast Wi-Fi Serving Self-Promotional Ads Via JavaScript Injection,* ARS TECHNICA, Sept. 8, 2014, http://arstechnica.com/tech-policy/2014/09/why-comcasts-javascript-ad-injections-threaten-security-net-neutrality/.

[34] Jacob Hoffman-Andrews, *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls,* ELECTRONIC FRONTIER FOUNDATION, Nov. 3, 2014, https://www.eff.org/deeplinks/2014/11/verizon-x-uidh.

[35] *See, e.g.*, TRAMMELL & KUEHLEWIND, IAB WORKSHOP ON STACK EVOLUTION IN A MIDDLEBOX INTERNET (SEMI) REPORT (2015), *available at* https://tools.ietf.org/html/draft-iab-semi-report-01.

[36] Michio Honda et al., *Is it Still Possible to Extend TCP*?, ACM INTERNET MEASUREMENT CONFERENCE 181 (2011), *available at* http://nrg.cs.ucl.ac.uk/mjh/tmp/mboxes.pdf.

sort of rapid innovation the Internet has fueled for the past two decades would come to a sudden and disastrous halt.

Fortunately, there is a way to prevent this worst-case scenario from occurring: uphold the FCC's Open Internet Order.

That is why we, the undersigned computer scientists, network engineers, and Internet professionals, based on our technical analysis and an understanding of both how the Internet was designed, how it currently functions, and what sort of technical changes ISPs are already making and wish to make in the future, respectfully encourage the Court to uphold the FCC's Open Internet Order.[37]

Respectfully submitted,

- Karl Auerbach, *Recipient of the Norbert Wiener Award from the Computer Professionals for Social Responsibility; Publicly elected Director, Internet Corporation for Assigned Names and Numbers (ICANN)* .
- Dr. Henry G. Baker, *Computer Scientist, Entrepeneur, Venture Capitalist; One of the founders of Symbolics, Inc., which held the first registered ".com" domain name*.
- Randy Bush, *Chair of the IETF Working Group on DNS for over a decade; recognized as a Global Connector by the Internet Hall of Fame*.
- Lyman Chapin, *Former Chair, Internet Architecture Board; former Chief Scientist, BBN Technologies*.

---

[37] Unless otherwise noted, all of the signatories to this letter have signed in their personal capacity, and not as representatives of their employers or any affiliated organizations.

- Professor Douglas Comer, *Distinguished Professor of Computer Science, Purdue University*.
- Owen DeLong, *Network Architect, Akamai Technologies and Member, ARIN Advisory Council*.
- Professor James Hendler, *Tetherless World Professor of Computer, Web and Cognitive Sciences, and Director, RPI Institute for Data Exploration and Applications, Rensselaer Polytechnic Institute*.
- Professor Nick McKeown, *Professor of Electrical Engineering and Computer Science, Stanford University; Member, National Academy of Engineering; Member, American Academy of Arts and Sciences*.
- Professor Scott Shenker, *Professor in Electrical Engineering and Computer Sciences Department, University of California-Berkeley; Member, National Academy of Engineering*.
- Eitan Adler, *Distributed Systems Engineer*.
- Eldridge Alexander, *Corporate Operations Engineer.*
- Sahle A. Alturaigi, *Cyber-security Analyst, Electronia (KSA)*.
- Bruce Artmant, *Systems Administrator, Acme Metal Works*.
- Jim Bauer, *Technology Leader*.
- Dovid Bender, *CTO, The Flat Planet Phone Company Inc.*
- Chris Boyd, *CTO, Midas Green Technologies*.
- Dave Brockman, *Senior Network Engineer, Networks Inc.*
- Gary Cohn, *Network Engineer*.
- Hugo Maxwell Connery, *Network Administrator, Technical University of Denmark; participant in the DNS Operations, DNS Private Exchange, and Pervasive Passive Surveillance IETF Working Groups*.
- Joshua Cox, *Systems Administrator*.

- Andrew Gallo, *Principal IT Architect*.
- Alfred Ganz, *Network Consultant*.
- Arthur S. Gaylord, *Director, Computer and Information Services, Woods Hole Oceanographic Institution, and President and Chairman of the Board, OpenCape Corporation*.
- Dr. Gregory Glockner, *Director of Engineering, Gurobi Optimization*.
- Plato Gonzales, *Blockchain Engineer and Electrical Engineer*.
- Joe Hamelin, *Network Engineer*.
- William Herrin, *Owner, Dirtside Systems*.
- Cristian Iorga, *Senior Software Engineer*.
- Valdis Kletnieks, *Computer Systems Senior Engineer, Virginia Tech*.
- Rich Kulawiec, *Senior Internet Security Architect, Fire on the Mountain, LLC*.
- Bob Mayo, *Computer Scientist since 1983; CTO, Researcher, and former Professor*.
- Andrew McConachie, *Internet Infrastructure Engineer*.
- Tim McGinnis, *Internet Governance Consultant*.
- Professor Joseph Meehean, *Assistant Professor of Computer Science, Lynchburg College.*
- Michael Meyer, *Senior Systems Specialist*.
- Gary E. Miller, *President, Rellim*.
- David M. Miller, *CTO and Executive Vice President of DNS Made Easy and Constellix*.
- Nicholas Oas, *Network Security Engineer*.
- Nick Pantic, *Computer Science Lecturer, Cal Poly Pomona*.
- Adam Rothschild, *Co-Founder and SVP, Infrastructure, Packet Host Inc.*

- Kent Schnaith, *Software Developer since 1978*.
- Nicholas Schrag, *Senior Engineer for client-side development of free-to-play mobile games*.
- Mark Seife, *Developer and Senior Database Administrator*.
- Tom Simes, *ISP Engineer; Started the first commercial Internet node in Northern Arizona in 1994*.
- Garry Star, *Senior Software Engineer*.
- Dr. Horst Tebbe, *Former member of the technical staff at Bell Labs*.
- Eric Tykwinski, *Network Administrator, TrueNet, Inc.*
- William K. Walker, *Owner, North Valley Digital*.
- Michael Weaklend, *Information Security Specialist*.
- Joel Whitcomb, *Network Engineer.*
- Nik Zorich, *Professional Network Engineer*.
- Aaron Zuehlke, *Senior IT Analyst--Application Security*.